EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
Facsimile: (732) 248-8273

BARTIMUS, FRICKLETON, ROBERTSON & GOZA, PC
715 Swifts Highway
Jefferson City, MO 65109
Telephone: (573) 659-4454
Facsimile: (573) 659-4460

Co-Lead Counsel on behalf of Plaintiffs

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

IN RE NICKELODEON CONSUMER PRIVACY LITIGATION	**No. 2:12-cv-07829 (SRC)(CLW)** **MDL No. 2443** **Judge Stanley R. Chesler**
This Document Relates to: **All Actions**	**PLAINTIFFS' OMNIBUS OPPOSITION TO THE MOTIONS TO DISMISS FROM DEFENDANTS VIACOM AND GOOGLE**

TO: Jeffrey J. Greenbaum
Joshua N. Howley
SILLS CUMMIS & GROSS, P.C.
One Riverfront Plaza
Newark, NJ 07102

Stephen M. Orlofsky
BLANK ROME, LLP
301 Carnegie Center, 3rd Floor
Princeton, NJ 08540

Colleen Bal
Michael Rubin
Tonia Klausner
WILSON SONSINI GOODRICH & ROSATI, PC
One Market Plaza
Spear Tower, Suite 3300
San Francisco, CA 94105

Bruce P. Keller
Jeffrey S. Jacobson
DEBEVOISE & PLIMPTON LLP
919 Third Avenue
New York, NY 10022

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

CASES **PAGE**

STATUTES

CODE OF FEDERAL REGULATIONS

SECONDARY AUTHORITY

INTRODUCTION

"THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection."

Samuel D. Warren, Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

Justice Louis Brandeis and Samuel Warren first conceptualized the American notion of an individual "right to privacy" in a Harvard Law Review article published in 1890. From this historical origin, the "right to privacy" has become firmly woven into the fabric of American jurisprudence, where it now finds expression in various common law doctrines, Federal and state statutes and even the opinions of United States Supreme Court Justices. *See Griswold v. Connecticut*, 381 U.S. 479, 486 (1965) ("We deal with a right of privacy older than the Bill of Rights—older than our political parties, older than our school system.").

But while the "right to privacy" has taken many forms before Congress and the Courts, those forms continue to share a common foundation. The "protection afforded to thoughts, sentiments, emotions, expressed through the medium of writing or arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the *more general right of the individual to be let alone*." *The Right to Privacy*, at 205 (emphasis added). "The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an *inviolate personality*." *Id.* at 206 (emphasis added). "The right of privacy concerns one's own peace of mind . . . ." *Fairfield*, 138 Cal.App.2d at 86.

The United States Supreme Court has also recognized that "children have a very special place in life which law should reflect." *May v. Anderson*, 345 U.S. 528, 536 (1953) (Frankfurter, J., concurring). Legal theories and their phrasing in other cases readily lead to fallacious

reasoning if uncritically transferred to determination of a State's duty towards children." *Id.* The Supreme Court has "recognized three reasons justifying the conclusion that the constitutional rights of children cannot be equated with those of adults: the peculiar vulnerability of children; their inability to make critical decisions in an informed, mature manner; and the importance of the parental role in child rearing." *Belotti v. Baird,* 443 U.S. 622, 635 (1979). Congress shares the Supreme Court's view, having enacted statutes providing children with additional, special legal protection concerning the "collection, use, and/or disclosure of personal information from and about children on the Internet." 15 U.S.C. § 6501, et seq. (the Children's Online Privacy Protection Act).

This case impacts the privacy rights of a nationwide class of minor children. Given the unprecedented progression of technological innovation that has occurred over the last two decades, Justice Brandeis and Mr. Warren's words remain pivotal. It is time once again to define anew the nature of children's right to privacy.

Defendants Viacom and Google, for their own pecuniary gain, have systematically employed Internet cookie technology to violate minor children's right to be let alone. Specifically, Defendants have developed third party cookies to share video-viewing histories of these children and otherwise to track the contents of the Internet communications of millions of American children. Defendants now seek dismissal, claiming what happened here was routine and consensual Internet practice. They miss the point. The statutory and decisional foundation that otherwise enables the Defendants to place cookies on user's computers is consent. Here, Defendants repeatedly ignore the fact that this is a class of children, who, as a matter of law, are incapable of providing consent. Put simply, minor children did not, and cannot consent to the monitoring of their communications and viewing histories. In light of the unique legal status of

these Plaintiffs, Defendants cannot conjure up a consent defense, nor find refuge in any other statute or common law doctrine from the consequences of their choice to engage in unlawful conduct.

Impliedly recognizing this, Defendants seek dismissal on the basis of decisions which do not fit these facts. Indeed, each and every Internet cookie related case cited by Defendants involved adult users. Defendants' theories of tacit or explicit consent do not withstand scrutiny when applied to minor children.

Nor is this case a "broadside attack on the use of cookies." Indeed, as illustrated by Plaintiffs' Master Consolidated Class Action Complaint ("Complaint"), not all cookies are created equal. Though first-party cookies may indeed be essential for how the Internet functions, third-party cookies are not essential for persons using the Internet. (Complaint ¶35(b)(2)). Instead, third-party cookies are used in furtherance of data collection, behavioral profiling, and targeted advertising (*i,e.*, for the pecuniary gain of the company that places them). *Id*. Third party cookies would certainly be permissible if their existence and use was conspicuously disclosed and agreed to by those capable of consent. But that is not the case here. Though Defendants would need to seek alternative means of generating revenue when it comes to minor children, the Internet would continue to function just fine without such tracking technologies forced upon children. The slippery slope is not as slick as the Defendants would have the Court believe.

As such, despite the studied efforts of Defendants to blur the distinction between first and third party cookies, Plaintiffs' claims are targeted and narrow, and designed to protect and vindicate the privacy rights of minor children. To be clear, Plaintiffs neither seek to upend progress, nor hamper innovation. Rather, they only seek to stop the unauthorized use of third-

party cookies to share the viewing habits and communications of minor children in violation of firmly embedded Federal law.

In sum, because their conduct has violated the statutorily protected privacy rights of children, Defendants have no statutory or common law refuge. Their conduct is neither consensual nor immunized, and their motions to dismiss should be denied because the Consolidated Complaint pleads facts establishing valid causes of action under the statutes and common law theories set forth therein.

STATEMENT OF FACTS

Plaintiffs' factual allegations are deemed true on a motion to dismiss. *Phillips v. City. of Allegheny*, 515 F.3d 224, 233 (3d Cir. 2008). Thus, any conflict between facts alleged in the Complaint and Defendant's attempts to present this Court with cherry-picked facts outside of discovery must be resolved in plaintiffs' favor. Defendants' motions to dismiss are almost entirely dependent upon the Defendant's interpretation of the facts, facts which are hotly disputed.

Plaintiffs are minor children under the age of 13 who are registered users of Viacom's children's websites: Nick.com, NickJr.com, and/or NeoPets.com (collectively "Viacom children's websites"). (Complaint ¶4). The Plaintiffs watched videos, played games and otherwise interacted on these websites. (Complaint ¶5). The Defendants utilized Internet technologies commonly known as "cookies" to track, share, and access the minor children's video-viewing histories and the content of their Internet communications on Nick.com, NickJr.com, NeoPets.com, and other non-Viacom websites without the Plaintiffs' consent.[1]

[1] "Cookies" are small Internet text files that web servers place on a person's computing device when that person interacts with a website. Complaint ¶33. Cookies are categorized by the party that sets them and the time they are designed to stay on a person's computer. Complaint ¶35.

(Complaint ¶¶5-6 (relating to general allegations); 128-130 (relating to VPPA); 137, 145, and 155 (relating to Wiretap Act); 165, 170, 172, and 173 (relating to SCA); 177 (CIPA); and 190 (N.J. Computer Related Offenses Act)).

Immediately upon the minor children Plaintiffs' first communication with Viacom's children's websites, Viacom: (1) placed its own first-party cookies on the minor children's computers; (2) knowingly permitted Defendant Google to place its own third-party cookies on the minor children's computers; and (3) upon information and belief, provided Google with access to profile and other information contained within Viacom's first-party cookies. (Complaint ¶¶73-74, 144). The placement of these cookies occurred before Plaintiffs or their guardians even had the opportunity to consent – or not consent – to their placement.[2]

First-party cookies are set by the actual website with which the person is intending to communicate. Complaint ¶35(b)(1). For example, Defendant Viacom placed first-party cookies on the computers of the minor children Plaintiffs to assist with security, log-in, and website functionality. *Id*. Third-party cookies are those which are set by websites other than the one with which a person intends to send a communication. Complaint ¶35(b)(2). For example, Defendant Google placed third-party cookies on the minor children Plaintiffs' computers on Viacom and non-Viacom websites. *Id*. Unlike first-party cookies, third-party cookies are not typically helpful to a person's use and communications on the Internet, but are instead used in furtherance of data collection, behavioral profiling, and targeted advertising. *Id*. Because advertising companies like Google serve advertisements and place corresponding cookies on multiple websites, their cookies also allow them to monitor a person's communications over every website and webpage on which the advertising company serves ads and places cookies. Complaint ¶47.

[2] Google's corporate headquarters are located in California. Complaint ¶178. Upon information and belief, as the location of Google's corporate headquarters, Google directed and used the tracking, access, interception, and collection of the plaintiffs' personal information and Internet communications in the state of California. Complaint ¶180. Because Google directed and used the behavior at issue in this case from California, every act of tracking and every interception took place, in part, in California, regardless of the particular location of each individual plaintiff. Complaint ¶181.

Next, Viacom encouraged the minor Plaintiff children visiting the Viacom children's websites to register as a user for each site. (Complaint ¶85).[3] During registration, Viacom obtained the child's birthdate and gender, to which it assigned an internal code name. (Complaint ¶¶86-97). Viacom also required the child to create a unique username in the sign-up process. (Complaint ¶90). Then, Viacom designed its code to allow Google to access each child's profile name and the code name for the child's specific gender and age. (Complaint ¶¶92-93). In total, for each child's registration, Viacom disclosed to Google the child's (1) username; (2) gender and birthdate combination; (3) IP address; (4) browser settings; (5) unique device identifier; (6) operating system; (7) screen resolution; (8) browser version; and (9) over time, the content of the child's web communications, including but not limited to the detailed URL requests and video materials requested and obtained from Viacom's children's websites. (Complaint ¶81). By assigning each minor Plaintiff a unique cookie identifier, Google was then able to associate the child's age, gender, and other information with the content of their communications, including the video materials they watched, transforming what would otherwise be a random set of URLs into a meaningful set of data connected to a particular individual to whom Viacom and Google could direct targeted advertising. (Complaint ¶94).

The Viacom children's websites are replete with videos and similar audio-visual materials. For example, Nick.com advertises itself as the place to watch "2000+ FREE ONLINE

[3] Viacom offers this Court a series of exhibits relating to the sign-up process. Though a large and critical portion of these exhibits comports exactly with the Complaint, this Court must reject Viacom's attempt to introduce cherry-picked evidence into the proceedings at this point.

To the extent Viacom's Exhibit contradicts Plaintiffs' Complaint with regard to the NickJr.com sign-up process, Plaintiffs note that the requirement of an email address and parental consent at the time of sign-up does not negate liability under the VPPA. For the relevant class period, "consent" under the VPPA must be "informed, written consent at the time the disclosure is sought." Complaint ¶118. If anything, Viacom's Exhibit on the NickJr.com sign-up process bolsters Plaintiffs' VPPA claim by adding another category of personally-identifiable information (email address) to the list Viacom provides to Google.

VIDEOS" and to "play 1000+ FREE ONLINE GAMES." (Complaint ¶126). NickJr.com advertises itself as the place to watch Dora the Explorer, Bubble Guppies and dozens of other children's shows. *Id*. NeoPets.com advertises itself as the place to play dozens of video games. *Id*. Google's third-party cookies are also used to track the specific video requests and viewing histories of minor children through the tracking of detailed URL requests that included the exact titles of the videos requested and received by the minor children. (Complaint ¶¶72-84). Through this tracking, Viacom knowingly disclosed, and Google knowingly obtained, the specific video and video-game requests and viewing histories of the Plaintiffs on the Viacom children's websites. (Complaint ¶¶70-78, 81-97, 122-124, 128-129).

In addition to tracking the content of Plaintiff children's communications on the Viacom children's websites, Google's cookies also tracked and recorded the content of Plaintiffs' communications immediately and continuously on non-Viacom websites without the consent of the Plaintiffs' or their guardians. (Complaint ¶¶145, 150-151, 155). Viacom knew or had reason to know that Google intentionally intercepted the content of the Plaintiffs' Internet communications with non-Viacom websites despite Google's knowledge that Plaintiffs' were minor children. (Complaint ¶158). Viacom procured Google to intercept the content of the Plaintiffs' communications with other websites, and, upon information and belief, profited from Google's unauthorized tracking on other sites as such information gleaned from the tracking assisted in the sale of targeted advertisements to the Plaintiffs on Viacom's children's websites. (Complaint ¶156-158).

Unbeknownst to the minor Plaintiffs, their web-browsers and computing devices are commandeered by Defendants to store cookie and other information on Plaintiffs' computers. (Complaint ¶¶166- 167). The Plaintiffs' web-browsers and computing devices are the software

and hardware necessary for and the items through which their electronic communications services are provided. (Complaint ¶¶169, 171). The Plaintiffs' web-browsers and computing devices are unwittingly forced to store cookie and other information on Plaintiffs' computers. (Complaint ¶¶169, 172). These cookies are updated regularly to record the contents of users' communications as they happen. (Complaint ¶172). In the process of tracking the contents of Plaintiffs' communications through unauthorized cookies, Google accesses these cookies to acquire profile information and the contents of just-transmitted user communications out of Plaintiffs' computers which is incidental to the transmission of the communications. (Complaint ¶172). Google's access to these unauthorized cookies began immediately upon Plaintiffs visiting the Viacom children's websites without the consent of the Plaintiffs or their guardians. (Complaint ¶170). Further, Google's access to the browser-managed files stored on Plaintiffs' computers was done without the authorization of the Plaintiffs' or their web-browsers or Internet Service Providers. (Complaint ¶168).

LEGAL ARGUMENT

I. PLAINTIFFS MEET ALL ARTICLE III STANDING REQUIREMENTS

This case involves an intrusion into the non-consenting minor Plaintiffs' right to privacy. When conducting a Rule 12(b)(1) analysis, "the Court accepts as true all material allegations set forth in the complaint, and must construe those facts in favor of the non-moving party." *Ballentine v. U.S.*, 486 F.3d 806, 808 (3d Cir. 2007). The Defendants urge this Court to tether Article III standing's injury-in-fact requirement to proof of economic loss, which the Defendants further argue Plaintiffs failed to plead sufficiently. Plaintiffs have adequately alleged standing for three reasons. First, the Plaintiffs have pled facts sufficient to establish statutory standing to sue under the Video Privacy Protection Act, Electronic Communications Privacy Act, Stored Communications Act, and various state statutes which do not depend on allegations of monetary

harm. Second, standing for privacy torts does not require such harm. And third, in any event, Plaintiffs adequately pled facts alleging monetary harm.

A. STANDING REQUIREMENTS

Article III standing consists of "(1) an injury-in-fact[4]. . . (2) a causal connection between the injury and the conduct complained of; and (3) that it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Winer Family Trust v. Queen*, 503 F.3d 319, 325 (3d Cir. 2007). A plaintiff must establish the elements of standing; however, "general factual allegations of injury resulting from the defendant's conduct may suffice." *Id.* (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992)). The test for standing is not demanding. *See Danvers Motor Co., Inc. v. Ford Motor Co., Inc.*, 432 F.3d 286, 291 (3d Cir. 2005) (Alito, J.) (emphasizing injury-in-fact's "very generous" contours and noting "[i]njury-in-fact is not Mt. Everest."). Nor does the strength or weakness of a case's merits have anything to do with standing. *Warth v. Seldin*, 422 U.S. 490, 500 (1975).

B. PLAINTIFFS HAVE STATUTORY STANDING

Injury-in-fact does not require "actual monetary damages, because 'the actual or threatened injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing." *Alston v. Countrywide Fin. Corp.*, 585 F.3d 753, 763 (3d Cir. 2009) (citing *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 373 (1982)) ("[c]ertainly, the fact that plaintiffs' injury is non-monetary is not dispositive" with respect to standing). For statutory standing, "the question" is simply whether the statutes under which the plaintiffs allege their claims "grant persons in the plaintiffs' position a right to judicial relief." *Warth*, 422 U.S. at

[4] Injury in fact requires damage to a legally protected interest which is (a) concrete and particularized and (b) actual or imminent as opposed to conjectural or hypothetical. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992)).

500. If plaintiffs are protected by the statute, they have standing to assert claims under the statute. *Id*. Viacom's Brief makes no mention of the binding precedent of the *Alston* case in urging that "it should join [the District of Illinois in] *Sherk* in holding that "[a] plaintiff must plead an injury beyond a statutory violation to meet the standing requirement of Article III." Viacom Motion to Dismiss at 21, n. 5.

Here, Plaintiffs pled statutory standing through an invasion of their conferred and codified rights under: (1) the Video Privacy Protection Act ("VPPA") (Complaint ¶¶ 115-132); (2) the Electronic Communications Privacy Act ("ECPA") (Count II, Complaint ¶¶ 133-160); (3) the Stored Communications Act ("SCA") (Count III, Complaint ¶¶ 161-174); (4) the California Invasion of Privacy Act ("CIPA") (Count IV, Complaint ¶¶ 175-187); and (5) the New Jersey Computer Related Offenses Act ("NJCROA") (Count V, Complaint ¶¶ 188-193).

It is well-settled law that plaintiffs who adequately allege violations of the VPPA, ECPA, SCA, and other statutory causes-of-action may establish standing based alone on allegations that a defendant violated the statutes. *See In re Hulu Privacy Litig.*, No. C11-03764 LB, 2013 WL 6773794 (N.D. Cal. Dec. 20, 2013) (Denying Defendant Hulu's Motion for Summary Judgment in case involving sharing of full-string URLs of video-viewing histories to third-parties. "Under the plain language of the [VPPA], Plaintiffs must show only a wrongful disclosure, and not an additional injury, to recover damages."); *Gaos v. Google*, No. 5:10-CV-4809, 2012 WL 1094646, at *3 (N.D. Cal. Mar. 29, 2012) (citing *Edwards v. First Am. Corp.*, 610 F.3d 514, 517 (9th Cir. 2010); *In re Google Inc. Street View Elec. Commc'n Litig.*, 794 F.Supp.2d 1067 (N.D. Cal. 2011) (Defendant Google does not challenge standing under Wiretap claim.).

C. PLAINTIFFS ALLEGE SUFFICIENT INJURY-IN-FACT THROUGH DEFENDANTS' VIOLATION OF THEIR RIGHT TO PRIVACY

Irrespective of economic loss, Plaintiffs suffered concrete injury the instant Defendants placed certain tracking cookies and began to monitor and record evidence of the Plaintiffs' communications on the Internet without their knowledge or consent. *See Fowler v. S. Bell Tel. & Tel. Co*., 343 F.2d 150, 155 (5th Cir. 1965). ("Publication or commercialization may aggravate, but the individual's right to privacy is invaded and violated nevertheless *in the original act of intrusion*.") (quoting *McDaniel v. Coca-Cola*, 2 S.E. 2d 810 (Ga. 1939)) (emphasis added); *see also Rhodes v. Graham*, 37 S.W.2d 46, 47 (Ky. 1931) ("[U]nwarranted invasion of the right to privacy constitutes a legal injury for which redress will be granted.").

In cases alleging intrusion upon a plaintiff's right to privacy, the injury materializes upon the intrusion itself because what was intended to remain private is no longer so. The right to privacy is "a most fundamental human right" and where threatened by "industrial espionage . . . the state interest in denying profit to such illegal ventures is unchallengeable." *Kewanee Oil Co. v. Bicron Corp*., 416 U.S. 470, 487 (1974). Thus, from a pleading standpoint, it is enough to allege intrusion alone. This is because "[t]he tort is *completed* with the obtaining of the information by improperly intrusive means." *Pearson v. Dodd*, 410 F.2d 701, 704 (D.C. 1969) (emphasis added).

In *Pearson v. Dodd*, the D.C. Circuit, thus, recognized this fundamental principle first espoused by Justice Brandeis and Samuel Warren nearly 80 years prior:

> Where there is an intrusion, the intruder should generally be liable whatever the content of what he learns. An eavesdropper to the marital bedroom may hear marital intimacies; or he may hear statements of fact or opinion of legitimate interest to the public; for purposes of liability that should make no difference.

Id. at 705. The very instant their unauthorized intrusion was accomplished, the Defendants had infringed upon the rights of Plaintiffs, causing a concrete *injury irrespective of whether that*

intrusion also caused monetary loss. Whether damages are capable of precise measurement "by a pecuniary standard is not a bar to [plaintiff's] recovery." *Rhodes*, 37 S.W.2d at 47.

Here, the right to sue for the intrusion into one's personal and private Internet communications, including one's browsing history, must be analyzed no differently – particularly when the individual was not even capable of consent. Plaintiffs, thus, did not have to allege the ability to monetize their Personally Identifiable Information ("PII") in order to plead facts establishing Article III standing. *See Fairfield v. Am. Photocopy Equip. Co.*, 138 Cal. App. 2d 82, 86 (Cal. App. Ct. 1955) (The legally enforceable right to privacy is "distinct in and of itself and not merely incidental to some other recognized right for breach of which an action for damages will lie."). As such, they have properly alleged facts establishing standing by virtue of allegations showing the Defendants' unlawful intrusion.

D. PLAINTIFFS ALLEGE SUFFICIENT ECONOMIC INJURY TO ESTABLISH INJURY-IN-FACT

Even though not required, Plaintiffs alleged facts showing economic harm. The Complaint alleges a violation of Plaintiffs' financial interests to support their allegations that personally identifiable information ("PII") has monetary value and is a commodity that companies – like Defendants – trade and sell. (Complaint ¶¶ 49-59.) At this pleadings stage, those allegations are deemed to be true. *Ballentine*, 486 F.3d at 810; *see also Del Vechhio v. Amazon, Inc.*, No. C11-366RSL, 2012 WL 1997697, at *2 (W.D. Wash. June 1, 2012); *Claridge v. RockYou*, 785 F. Supp.2d 855, 861-62 (N.D. Cal. 2011).

E. DEFENDANTS' CASES ILLUSTRATE WHY THIS CASE IS DIFFERENT

Both Defendants rely on *Del Vechhio v. Amazon* and *LaCourt v. Specific Media* to support the spurious argument that courts have rejected standing in cases like this. In *Del Vecchio*, the plaintiffs alleged privacy violations against a defendant website for tracking the

communications of adult plaintiffs and which the defendant Amazon.com clearly disclosed prominently on its own website. Unlike the plaintiffs in *Del Vechhio*, this case involves minor children who are incapable of consenting to Internet tracking. Here, there is no claim of wrongdoing on the part of Defendant Viacom for tracking its own communications with the minor Plaintiffs. Rather, Plaintiffs' claims revolve around the unlawful disclosure of those communications to third-parties and the tracking of the minor Plaintiffs on non-Viacom websites. *Del Vecchio* is thus inapposite.

Nor is *LaCourt* on point. There, the plaintiffs did not allege they were personally affected by defendants' practices violating specific statutes, making only "tepid" and "half-hearted" harm allegations. *LaCourt v. Specific Media*, No. 10-1256-GW, 2011 WL 1661532, at *4-5 (C.D. Cal. April 28, 2011). They "more or less completely accepted Defendants' framing of the issue." *Id.* at *4. The *LaCourt* panel said it "probably would decline to say that it is categorically impossible for Plaintiffs to allege some property interest that was compromised by Defendant's alleged practices . . . [but] at this point they have not done so." *Id.*

Here, Plaintiffs are all minor children who are registered users of Viacom's children's websites. They allege that the content of their communications were illegally disclosed, intercepted, and tracked by the Defendants. Moreover, Plaintiffs adequately and specifically pled economic damages as a result of those privacy intrusions. (Complaint ¶¶ 49-59.)

F. PLAINTIFFS' ADEQUATELY PLED FACTS SUFFICIENT TO ESTABLISH STANDING

The Defendants' standing arguments ask this Court to eviscerate the ability of ordinary plaintiffs to sue to defend their "fundamental human right" to privacy as established through specific statutes and over 100 years of common law. Defendants' arguments to the contrary, plaintiffs who allege violations of statutes have standing to vindicate the rights created by those

statutes. Moreover, American courts have consistently found that standing is created for privacy torts based on the intrusion alone. Plaintiffs here, all minor children, have pled sufficient facts to establish statutory and privacy standing. In addition, they have pled sufficient facts to establish standing for economic loss. As such, this Court should find that the Consolidated Complaint satisfies Rule 12(b)(1).

II. PLAINTIFFS STATE VALID CLAIMS IN THEIR COMPLAINT

A. LEGAL STANDARD

A complaint must contain sufficient factual matter to "state a claim for relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Bell Atlantic Corp v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that discovery will reveal evidence of the misconduct alleged. *Phillips*, 515 F. 3d at 254 (quoting *Twombly*, 550 U.S. at 556). All well pled factual allegations are accepted as true and viewed in the light most favorable to the plaintiff. *Ballentine*, 486 F.3d at 810. "Further, [t]he 'issue is not whether a plaintiff will ultimately prevail but whether he or she is entitled to offer evidence to support the claims.'" *Id.* (internal citation omitted). Where an amended pleading could cure a deficiency in a complaint, the Third Circuit Court of Appeals requires District Courts to grant leave to amend, even where such relief is not sought. *Shane v. Fauver*, 213 F.3d 113, 116 (3rd Cir. 2000).

B. PLAINTIFFS STATE A VALID CLAIM UNDER THE VPPA AS TO VIACOM

Viacom takes great pains to shroud its conduct in various levels of abstraction in the hope that it can confound the Court, and frustrate the objectives of the VPPA. However, Viacom's violations of the VPPA are continuous, persistent and very real.

Viacom maintains that Plaintiffs have failed to allege a cognizable violation of the VPPA because Plaintiffs have not alleged the disclosure of PII. This is simply not true. Plaintiffs allege the precise disclosure contemplated by the VPPA, in that Viacom, in addition to disclosing video viewing histories of its users to a third party, Google, has also disclosed the Plaintiffs' usernames, gender, unique identifiers, IP addresses, and other PII that identifies each of these minor users on the Viacom children's websites.

The VPPA was intended by Congress to be a new type of privacy protection for "an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers . . . ." S. Rep. No. 100-599 at 6 (1988); *see also Dirkes v. Borough of Runnemede*, 936 F.Supp. 235, 238-39 (D.N.J. 1996) (quoting Senator Leahy comments). In discussing the VPPA, Senator Leahy specifically noted that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance. S. Rep. No. 100-599 at 7. Indeed, Senator Leahy noted that with such information:

> [I]t would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone. * * * I think that is wrong. I think that really is Big Brother, and I think it is something that we have to guard against.[5]

Id. at 6. The VPPA makes clear that "the term 'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services." 18 U.S.C. § 2710(a)(3). This is an expansive definition that includes *any* information that ties a particular person to a particular film. *See* S. Rep No. 100-599 at 7 ("[t]he bill prohibits . . . [the disclosure of] 'personally identifiable

information' – information that links the customer or patron to particular materials or services."). Viacom cites no binding authority to support its narrow definition of what qualifies as PII covered by the VPPA.[6] Nothing in the Congressional record or the definition of PII itself suggests such a narrow scope.

Courts have long found PII to extend far beyond a user's actual name and address. *See In re Hulu Privacy Litigation*, No. C11-03764, 2012 WL 3282960, at *2 (N.D. Cal. August 10, 2012) ("*Hulu II*"). This is because courts must construe the VPPA broadly to effectuate the actual intent of Congress. *See, e.g.*, *Dirkes*, 936 F.Supp. at 239 ("in construing the scope of the Act, this Court must strive to protect this aspect of an individual's right to privacy in the face of technological innovations that threaten this fundamental right.") In *Hulu II*, the Court found PII under the VPPA extended to Facebook IDs, "Hulu profile identifiers," and "Hulu username[s] (which, in the case of many individuals, is the same screen name used in other online environments)." *Hulu II*, 2012 WL 3282960, at * 2. In denying Hulu's motion to dismiss under Fed. R. Civ. P. 12(b)(6), the Court in *Hulu II* found that such disclosure of this type of information to third-party advertisers fell within the ambit of the VPPA. *See Id*. The information disclosed by Viacom to Google is akin to that disclosed by Hulu. It is personally identifiable information as the VPPA contemplates.

---

[6] Viacom claims that no information they have disclosed, including anonymized or psuedenonomized information, can tie a person to their real-world identity. That is merely a fiction. Such assigned "anonymous" information by Viacom can actually be far more likely to lead directly to a specific person. Disclosing that a real-world John Smith watched "Pocahontas" would lead one to a large group of people across the country. User ID numbers, however, have led to the identification of individual people with uncanny accuracy. *See* Michael Barbaro & Tom Zeller, *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, *available at* http://www.nytimes.com/2006/08/09/technology/09aol.html (detailing the simple identification of a person who used America Online's search tool from her search history and user ID number).

Ignoring this Court's holding in *Dirkes*, and the Third Circuit's holding in *Alston*, Viacom suggests this Court instead should follow the Third Circuit's interpretation of a completely different statute, the Drivers Privacy Protection Act ("DPPA"), in order to find that it did not disclose PII under the VPPA. *See Pichler v. UNITE*, 542 F.3d 308 (3d Cir. 2008). While the DPPA's language that enables a civil action is similar in some ways to the VPPA, the DPPA's definitions of "personal information" and "highly restricted personal information" are very different from how the VPPA defines PII. *Compare* 18 U.S.C. §§ 2721, 2725 *with* 18 U.S.C. § 2710; *see In re Hulu*, 2013 WL 6773794, at *7 ("*Hulu III*") (finding that the DPPA and VPPA "differ in their description of . . . protected personal information"). The DPPA specifically enumerates personal information related to a driver that is protected, while the VPPA intentionally uses a broader definition. *Id*. Moreover, the DPPA classifies the information to be protected in a spectrum, while the VPPA affords all PII the same protections. *Id*. Thus, the interpretation of the Third Circuit of the DPPA should not guide this Court's interpretation of the VPPA.[7]

Similar to the DPPA, and unlike the broad definition contained in the VPPA, the Children's Online Privacy Protection Act, 18 U.S.C. § 6501, et. seq., ("COPPA") specifically enumerates the "personal information" of children protected by the Act. However, COPPA contains a broad catch-all in the definition – allowing that "personal information" shall include "any other identifier that the [Federal Trade Commission] determines permits the physical or online contacting of a specific individual." *See id*. at § 6501(8)(F). Tasked with analyzing the definition of personally identifiable information in an increasingly interconnected and online

[7] Similarly, Viacom's citation of *Johnson v. Microsoft Corp.*, No. C06-0900RAJ, 2009 WL 1794400, (W.D. Wash. June 23, 2009), is inapposite. *Johnson*, involves the interpretation of an undefined term within a private contract. *See Johnson*, 2009 WL 1794400 at *2.

world, the Federal Trade Commission has determined that personal information "means *individually identifiable information* about an individual collected online, including:

> (3) Online contact information as defined in this section;[8]
> (4) A screen or user name where it functions in the same manner as online contact information, as defined in this section; …
> (7) A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier; …
> (10) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

16 C.F.R. § 312.2 as published in Vol. 78, No. 12 of the Federal Register on January 17, 2013[9] These statutes and regulations further demonstrate that Plaintiffs have properly alleged the dissemination of PII in this case.

If the Court seeks additional authorities for the conclusion that usernames and persistent identifiers constitute personally identifiable information, it should look to the statements and actions of the Defendants themselves, who have engaged in a long-running battle over Viacom's claims that Google is violating Viacom copyrights on YouTube.com. *See Viacom Int'l, Inc. v.*

---

[8] "Online contact information" is defined as "an email address or any other substantially similar identifier that permits direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over Internet protocol (VOIP) identifier, or a video chat user identifier.

[9] The Commission explained:
The Commission continues to believe that persistent identifiers permit the online contacting of a specific individual. As the Commission stated in the 2011 NPRM, it is not persuaded by arguments that persistent identifiers only permit the contacting of a device.
Nor is the commission swayed by arguments noting that multiple individuals could be using the same device. Multiple people share the same phone number, the same home address, and the same email address, yet Congress still classified those, standing alone, as "individually identifiable information about an individual." For these reasons, and the reasons stated in the 2011 NRPM, the Commission will retain persistent identifiers within the definition of personal information. *Children's Online Privacy Protection Rule*, 78 Fed. Reg. 12, 3980 (January 17 2013) (available at: http://www.gpo.gov/fdsys/pkg/FR-2013-01-17/pdf/2012-31341.pdf).

Youtube, Inc., USDC SD NY Case No. 1:07-cv-02103. In that litigation, a discovery issue arose over whether Google should be required to disclose to Viacom the usernames and IP addresses of YouTube users connected to those same users' video viewing histories. Following public outcry over a court ruling requiring such disclosures, the Defendants agreed that usernames and IP addresses were personally identifiable information that had to be shielded from discovery. As explained by Viacom:

> A recent discovery order by the Federal Court hearing the case of *Viacom v. YouTube* has triggered concern about what information will be disclosed by Google and YouTube and how it will be used. Viacom has not asked for and will not be obtaining any *personally identifiable information* of any YouTube user. The *personally identifiable information* that YouTube collects from its users will be stripped from the data before it is transferred to Viacom.[10]

The Defendants then stipulated that YouTube would produce information but would use "substitute values" for User IDs, IP Addresses, and Visitor IDs – a list which is not as broad as that which Plaintiffs have alleged constitutes personally identifiable information here.[11] Viacom and Google rightfully took steps to protect the personally identifiable information of YouTube video viewers during their internal dispute,, and this Court should hold them to that same standard here.

Thus, despite Viacom's misguided attempts to re-cast Plaintiffs' allegations of improper disclosure of PII under the VPPA, Plaintiffs' Complaint alleges that Viacom collected a minor child's username, gender, birthdate, unique identifier, operating system, settings of the browser, screen resolution, browser version, and other individual and unique information that it then

---

[10] Viacom Statement on Confidentiality of YouTube Data – 7/7/2008, available at http://news.viacom.com/news/Pages/youtubeconfidentiality.aspx as of Feb. 16, 2014.

[11] *See* Stipulation Regarding July 1, 2008 Opinion and Order, *Viacom International, Inc. v. YouTube and Google* (USDC SD NY Case No. 1:07-cv-02103) (Filed 3/13/07) Civil Docket No. 119.

disclosed to Google. (Complaint. ¶¶ 70-78, 81-90, 122-124). Nowhere does Viacom attempt to contest these factual assertions, which must be taken as true at this juncture.

Though Viacom may argue that some of this information, when viewed in isolation and independent of the whole, may not qualify as PII, when this information is taken together, and viewed in its totality,[12] it creates a vivid and specific portrait of the user. From this information, Google knows a child's username, sex, age, type of computer, and exact location.[13] Indeed, this PII was paired by Viacom along with the video materials specifically requested by the child to identify the child.[14] (Complaint ¶¶ 70-79, 97, 122-124). Using this information, Google was able to target specific children with advertisements it deemed relevant based on the PII it received from Viacom. (Complaint ¶ 80, 97, 122-124). All of this was done without the user's consent. (Complaint ¶ 98, 124).

Viacom's feeble effort to restrict the scope of the VPPA's reach only to those who disseminate "prerecorded video cassette tapes," Viacom Motion to Dismiss at 19, n.4, ignores that Congress envisioned technological advancements in the distribution of video media in drafting the statute. Rejecting a similar argument, this Court observed:

---

[12] *See, e.g, In re Neurontin Antitrust Litig*., No. 02-1390, 2009 WL 2751029, at *11-12 (D.N.J. Aug. 28, 2009) (holding, in the antitrust context, that "injuries arguably inflicted by [Defendant's conduct] should, instead, be viewed as a whole.") (*citing Biovail Corp., Int'l v. Hoechst AG*, 49 F.Supp. 2d 750, 767 (D.N.J. 1999) ("Again, this court will not evaluate whether each and every anticompetitive act … directly caused [Plaintiff's] injury. Instead, it will determine whether [Plaintiff] was injured by the anticompetitive conduct as a whole . . . .").

[13] IP addresses are looked up easily to reveal geolocation information. *See IP Details for 50.243.48.166*, http://whatismyipaddress.com/ip/50.243.48.166 (revealing the country, state, city, latitude, longitude, area code, and postal code for IP Address 50.243.48.166, one of the computers utilized by plaintiffs' counsel in preparation of this brief).

[14] Contrary to Viacom's suggestion that Plaintiffs have failed to plead with specificity that Viacom disclosed the videos watched by Plaintiffs, Plaintiffs have indeed alleged that information regarding every video watched by every user was sent to Google with specific information to identify the individual watching the video. (Complaint ¶¶ 70-78, 81-97, 122-124.)

> Because the Defendants are not video tape service providers as that term is defined under the Act, they argue they cannot be held responsible under the Act.
>
> This Court must reject Defendants' narrow reading of the statute. Again, the plain language of the Act does not delineate those parties against whom an action under this Act may be maintained. Taking the Defendants' argument to its logical extension, this omission would prevent plaintiffs from bringing a cause of action against anyone. Such an absurd result must be rejected. The clear intent of the Act is to prevent the disclosure of private information. As established by its legislative history, the Act enables consumers "to maintain control over personal information divulged and generated in exchange for receiving services from video tape service providers." This purpose is furthered by allowing parties, like these Plaintiffs, to bring suit against those individuals who have come to possess (and who could disseminate) the private information in flagrant violation of the purposes of the Act. While it need not identify all potential categories of defendants in this opinion, the Court finds that those parties who are in possession of personally identifiable information as a direct result of an improper release of such information are subject to suit under the Act.

Dirkes, 936 F.Supp. at 239-40. To combine the above-described PII with a user's video viewing history is exactly the type of tracking that concerned Congress when it drafted the VPPA.[15] This is "information that links the customer or patron to particular materials or services" and allows for a "subtle and pervasive form of surveillance." S. Rep. 100-599 at 7. This surveillance by Viacom (an individual who could disseminate PII) is sent to Google (an individual who has come to possess PII) and used to send a specific person (in this case, Plaintiffs who are minor children) specific advertisements, in violation of the VPPA. Thus, it furthers the purpose of the VPPA to allow parties, like the Plaintiffs here, to sue both Viacom and Google for unauthorized dissemination of their PII. Plaintiffs should be deemed to have adequately stated such claims in view of their factual allegations about what Viacom and Google have done.

[15] Indeed, the court in *Hulu II* correctly held that the VPPA applied to online video streaming. *See Hulu II*, 2012 WL 3282960, at *4-5.

C. PLAINTIFFS STATE VALID CLAIMS UNDER THE VPPA AS TO GOOGLE

Plaintiffs have also asserted valid claims against Google for their violation of the VPPA. First, Plaintiffs state a claim against Google for a violation of the VPPA's disclosure provision. Second, Plaintiffs state a claim against Google for failing to destroy the PII it illegally received. Google nonetheless argues, in contravention to District of New Jersey precedent, that the facts alleged here do not give rise to liability. For the reasons set forth below, this Court should follow the law of this district and deny Google's Motion to Dismiss because Google has violated the clear terms of the VPPA.

1. Google is a Properly Named Defendant

Google is a proper Defendant for a disclosure claim under the VPPA as it is in possession of illegally obtained PII. Parties "who are in possession of personally identifiable information as a direct result of the improper release of such information are subject to suit under the [VPPA]". *Dirkes*, 936 F.Supp. at 240. In *Dirkes*, the plaintiffs brought a claim against a police officer, his police department, and the Borough, which received illegally obtained PII and a video rental history from a video store. *Id*. at 236. This Court held that, even though they did not disclose the information, the police officer, the police department, and the Borough were proper parties because they possessed PII paired with a video rental history. *Id*. at 240. The Court reasoned that among the relief available to plaintiffs under the VPPA are equitable remedies. 18 U.S.C. 2710(c)(2)(D), *Dirkes*, 936 F.Supp. at 239. In order to effectuate the VPPA's purpose, which is to protect an individual's private information, possessors of illegally obtained information must be able to be hauled into court to prevent further disclosure. *Dirkes* 936 F.Supp. at 241.

Here, as in *Dirkes*, Plaintiffs allege that Google has illegally received their PII, along with their video viewing histories, from Viacom in direct violation of the VPPA. (Complaint ¶¶

70-98, 122-126). Like the plaintiffs in *Dirkes*, the Plaintiffs here should be able to seek the remedies available to them under the VPPA to prevent further disclosure of their information.

2. Plaintiffs Have a Valid Claim Against Google for Its Failure to Destroy Records Containing Personally Identifiable Information

Plaintiffs also state a claim under the VPPA against Google for failure to destroy illegally obtained PII. First, there is a private right of action for violations of 18 U.S.C. § 2710(e). Second, Google is a "video tape service provider" ("VTSP") as defined by the VPPA and by virtue of its receipt of PII. Finally, Google retained PII longer than allowed by 18 U.S.C. 2710(e). Accordingly, this Court should allow Plaintiffs' claims against Google to proceed.

a. The VPPA Provides a Private Right of Action to Plaintiffs

There is a private right of action for the failure to destroy records as required by the VPPA. The VPPA authorizes "[a]ny person aggrieved by any act of a person in violation of this section [to] bring a civil action in a United States district court." 18 U.S.C. § 2710(c)(1). Subsection (e) demands that persons "subject to this section *shall* destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected." 18 U.S.C. § 2710(e) (emphasis added). Section 2710 thus establishes a deadline for the destruction of PII, and a civil remedy for the violation of the requirements of the Section. To hold otherwise would disregard the plain meaning of the statute, as well as Congress' intent in safeguarding an individual's PII.

Indeed, courts have held that violations of subsection (e) are actionable under subsection (c). *See Dirkes*, 936 F.Supp. at 239 ("a person subject to the Act violates § 2710(e) by failing to timely destroy a customer's personally identifiable information"). To dispute this precedent, Google points to outside authority, *Sterk v. Redbox Automated Retail, LLC*, 672 F.3d 535 (7th

Cir. 2012), and *Daniel v. Cantrell*, 375 F.3d 377 (6th Cir. 2004). However, neither decision is persuasive.

The *Sterk* Court held only that a plaintiff could not maintain a claim for damages against a violator of subsection (e).[16] *Sterk*, 672 F.3d at 539. It left open the possibility that a plaintiff could seek equitable relief for a violation of subsection (e). Indeed, such a claim has proceeded to summary judgment. *See Sterk v. Redbox Automated Retail, LLC*, No. 11-C-1729, 2013 WL 4451223, at *6 (N.D. Ill. Aug. 16, 2013). Thus, *Sterk* does not support Google's Motion to Dismiss.[17]

Daniel is similarly inapposite. In *Daniel*, the Sixth Circuit analyzed whether a violation of subsection (d) was actionable under subsection (c). *Daniel*, 375 F.3d at 385. The *Daniel* court chose to ignore the plain language of subsection (c), which creates a cause of action for "any act . . . in violation of [§ 2710]," and instead concluded that "only § 2710(b) can form the basis of liability." *Id.* This case stands in stark contrast to the proper interpretation of the VPPA in the District of New Jersey. *See, Dirkes*, 936 F.Supp. at 239. In this District, *any* violation of subsections 2710(b), (d), or (e), allows a party to bring a private cause of action against the offending party. *Id.* Accordingly, Plaintiffs claims for both damages and equitable relief should be permitted to proceed.

[16] Unlike the Third Circuit, the Seventh Circuit does not recognize the availability of liquidated damages provisions, like those contained in the VPPA. *Compare Sterk*, 672 F.3d at 538-539, *with Pichler v. UNITE*, 542 F.3d 30, 398-400 (3d Cir. 2008), *and Hulu III*, 2013 WL 6773794 at *7-8. The subsection (e) claims in *Sterk* were brought against the party which collected the PII, not to whom it was disclosed. *Sterk*, 672 F.3d at 536.

[17] Notably, there was no disclosure in *Sterk*, which implicated subsection (e). In other words, there was no allegation that Red Box disclosed information and that information was unlawfully retained by Google. Here, Plaintiffs claim both unlawful disclosure to Google and unlawful retention by Google.

b. Google is a Video Tape Service Provider as Defined by the VPPA

Google further maintains that it is not a proper Defendant because it is not a VTSP. This is simply untrue. Even if this was required for a violation of the VPPA, and it is not, contrary to Google's assertions, it is in fact a VTSP within the meaning of the VPPA. 18 U.S.C. § 2710(a)(4); *Dirkes*, 936 F.Supp. at 240-41. The VPPA defines a VTSP as:

> [A]ny person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

18 U.S.C. § 2710(a)(4).

For Google to maintain that it is not a VTSP is absurd. In its description of itself, Google notes:

> In 2006, we acquired online video sharing site YouTube. Today 60 hours of video are uploaded to the site every minute. Cat videos, citizen journalism, political candidacy and double rainbows have never been the same.

Google, *About Google: Company, Broadcast Yourself*, http://www.google.com/about/company.[18]

By Google's own admission, the company is "engaged in the business . . . or delivery of . . . audio visual materials." *Id*. Online video services, like YouTube, are considered to be VTSPs within the meaning of the VPPA. *Hulu II*, 2012 WL 3282960, at *4-*6.

Google asserts that it also does not fit within the alternate definition of (a)(4). For the sake of argument only, as Google falls plainly within the definition of a VTSP, even if this Court determines that Google is not a VTSP by virtue of its operation of YouTube, it is undisputed that

[18] "This webpage is properly considered here because it is incorporated by reference into the complaint." Google Br. at 30 n. 10 (*citing Edelman v. Croonquist*, No. 09-1938, 2010 WL 1816180, at *4 n. 1 (D.N.J. May 4, 2010)).

Google has received information from another VTSP, Viacom, within the meaning of § 2710(a)(4). Notably, Viacom does *not* contest its status as a VTSP. *See generally* Viacom Motion to Dismiss. Any PII Google received from Viacom, illegal or not, would cause it to be a VTSP within the meaning of the VPPA and subject it to the Act's destruction requirements. *See* 18 U.S.C. § 2710(a)(4), (e).

c. Google Violated the VPPA by Retaining Personally Identifiable Information Longer than Necessary

Google was not authorized to receive *any* PII from Viacom. As such, PII retained by Google was retained in violation of subsection (e). 18 U.S.C. 2710(e). In its report on the VPPA, the Senate made clear that "the phrase 'the purpose for which it was collected' [within subsection (e)] must be narrowly construed." S. Rep. No 100-599 at 10. Moreover, the "purpose" cannot "include activities that violate the intent of the statue, which is to protect personally identifiable information from disclosure." *Id*. In other words, Congress did not intend for a party in illegal receipt of PII to be able to retain it legally. Therefore, the Plaintiffs need not allege that their PII was retained for any specific period of time. Google had an obligation to destroy the information as soon as practicable, or in other words, immediately upon receipt.

Plaintiffs allege that Google received PII including information that ties a specific user to a specific video viewed. (Complaint ¶¶ 70-78, 81-97, 122-126). Plaintiffs aver that Google does not destroy this information, but instead retains it to build a profile on a particular person and target them with specific advertisements. *Id*. It would be contrary to Google's practices to destroy this data. (*Id*. at ¶¶ 31-47, 68-69, 149). Plaintiffs believe Google has continued to illegally retain a database of this illegally obtained PII, but only through this action can Plaintiffs

obtain the discovery necessary to stop these practices by Google. *Id.* For all of these reasons, Plaintiffs' claims against Google for statutory damages and equitable relief should proceed.

D. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT IS APPLICABLE TO THE ACTIONS OF BOTH DEFENDANTS AND PLAINTIFFS STATED VALID CLAIMS UNDER THAT ACT

In 1986, the Electronic Communications Privacy Act ("ECPA"), set forth in 18 U.S.C. § 2510, *et seq.*, "amended the Federal Wiretap Act by extending to data and electronic transmissions the same protection already afforded to oral and wire communications." 132 Cong. Rec. S14441-04, 1986 WL 786307 (1986). The paramount objective of the Act "is to protect effectively the privacy of communications." *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003). (internal citation omitted).

To state a claim under the ECPA, the plaintiff must allege the defendant: (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device. *Id*. at 18.

1. The ECPA Applies to 1st and 3rd Party Cookies Such as Those Used by Defendants Viacom and Google Respectively

Defendants claim the ECPA does not apply to first or third party cookies in this case because it is a single party consent statute and Viacom consented to the disclosure. First, consent is an affirmative defense the defendants bear the burden of establishing. Thus, it is not the proper subject for a Motion to Dismiss. Moreover, Defendant's arguments are incorrect for two reasons. First, the statute specifically notes that party consent is irrelevant when "such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any state." 18 U.S.C. § 2511(2)(d). Second, Viacom's consent is irrelevant in this matter because the communication involved minors, who did not, and could not consent here.

a. Defendants' Criminal and Tortious Acts Make Their Consent Irrelevant and the ECPA Applicable to Their Actions in Illegally Tracking Plaintiffs

Defendants attempt to use the ECPA as a shield from liability by claiming that Viacom and Google's respective consent to disclosure relieves both Defendants of liability under the ECPA. Viacom Motion to Dismiss at 26; Google Motion to Dismiss at 17. The exception to consent rule is inapplicable here because it was the Defendants' intention to violate multiple Federal and State laws. 18 U.S.C. § 2511.

Defendants attempt to show that multiple cases hold that this exception to the consent rule is exceedingly narrow and should not apply. See Google Motion to Dismiss at 18; Viacom Motion to Dismiss at 28. This proposition is incorrect, however, as the plain language of the statute is unambiguous in merely requiring that "such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any state." 18 U.S.C. § 2511(2)(d). Even the case upon which Viacom principally relies, *In re DoubleClick Inc. Privacy Litig.*, cites with approval a 9th Circuit case that holds: "For this [Wiretap] claim to survive . . . [Plaintiff] had to come forward with evidence to show that [the defendant] taped the conversation . . . *for the purpose of invading her privacy* . . . . The record is devoid of any such evidence." *In re DoubleClick Inc. Privacy Litig.*, 154 F.Supp.2d 497, 516 (S.D.N.Y. 2001) (citing *Detersa v. ABC*, 121 F.3d 460 (9th Cir. 1997)).

This case is distinguishable from *DoubleClick* because Plaintiffs have pled that Defendants' "scheme to track the Plaintiffs' Internet communications . . . intentionally intruded upon the Plaintiffs' solitude or seclusion in that Defendants took information from the privacy of the Plaintiffs' homes." (Complaint ¶195). Thus, under *DoubleClick*, Plaintiffs' allegation of

intrusion upon seclusion is sufficient to invoke the tort/crime exception of the ECPA, and negate the relevance of Viacom's consent.

Alternatively, at least one court in the third circuit has held that violating § 2511(1)(c) operates to negate single party consent. *See, L.C. v. Central Pa. Youth Ballet*, No. 1:09-cv-2076, 2010 WL 2650640, at *3 (M.D. Pa. July 2, 2010) (denying defendant's motion to dismiss and holding intentional disclosure to third party violates ECPA and second violation negates single party consent bringing exception into play). § 2511(1)(c) provides it is illegal for one who "intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication . . ." 18 U.S.C. § 2511. The net result is multiple violations of the ECPA: (1) the interception of Plaintiffs' data; and (2) the disclosure of Plaintiffs' data to a third party – here, Viacom's disclosure to Google. Viacom always intended to allow for the disclosure of Plaintiffs' information to Google. *See* Viacom Motion to Dismiss at 30 (describing Google's cookie placement as "authorized"). Viacom's separate and distinct intentional disclosure in violation of the ECPA negates the consent argument and brings the exception to the consent rule into play.

b. Defendants' Consent is Irrelevant Because Plaintiffs are Minors

Defendants contend that the age of the minor Plaintiffs is irrelevant because the ECPA is a single party consent statute. However, a minor's ability to contract and consent to an agreement has never been treated in the same way as an adult. The age of a minor is "more than a chronological fact." *Eddings v. Oklahoma*, 455 U.S. 104, 115 (1982). "It is a fact that generates commonsense conclusions about behavior and perception." *J.D.B. v. North Carolina*, 131 S.Ct. 2394, 2404 (2011) (internal citation omitted). The Supreme Court has reiterated this

concept repeatedly and unequivocally. *See e.g.*, *Bellotti*, 443 U.S. at 635 (plurality opinion) (Children "often lack the experience, perspective, and judgment to recognize and avoid choices that could be detrimental to them"); see also *Gall v. U.S.*, 552 U.S. 38, 58 (2007); *Roper v. Simmons*, 543 U.S. 551, 569 (2005); *Johnson v. Texas*, 509 U.S. 350, 367 (1993).

It is a basic tenet that interactions involving minors cannot be held to the same standard as those between two adults. If Defendants' argument is successful, the net result is that they will have been permitted to violate the ECPA and invoke an exception by taking advantage of minor children who lacked any legal capacity to understand what happened. Plaintiffs suggest the better rule is that "when one party to a conversation is under the age of eighteen, the *only* person who can consent to an interception is a . . . judge" or parental guardian. *Bishop v. State*, 241 Ga.App. 517, 522 (1999) (emphasis in original).

2. Defendants' Interception of URLs, IP addresses, Birthdates and Gender are "Contents" under the ECPA

Broadly defined under the ECPA, "contents" "includes *any* information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8) (emphasis added). This definition governs both Title I to the ECPA (the Wiretap Act), and its reciprocal counterpart – Title III to the ECPA (the Pen Register Act).[19]

Plaintiffs' Complaint notes that Defendants' cookies violated Federal and State laws in disclosing personal information about the minor Plaintiffs including, but not limited to, their gender, birthdate, IP address, and web communications through specific URL requests. Complaint at ¶¶81-82. What qualifies as "contents" under the ECPA is largely a factual

[19] Combined, the Wiretap and Pen Register Acts cover all aspects of a communication. The Wiretap Act prohibits the interception of "contents" and the Pen Register Act prohibits the recording of non-content "dialing, routing, addressing, or signaling information. (DRAS)" 18 U.S.C. § 3127(3). As explained herein, URLs contain both content and signaling information.

question. The term "contents" is broad, including "*any* information *about* the substance, purport or meaning" of a communication.

a. URLs are "Contents" Under the ECPA

Broadly defined under the ECPA, contents "includes *any* information concerning the substance, purport or meaning of [a] communication." 18 U.S.C. § 2510 (8). A URL satisfies this definition because URLs can often convey the substance, purport and meaning of a communication. *Declassified Opinion from the United States Foreign Intelligence Surveillance Court*, (date redacted) ("*FISC Opinion*") (attached as Exhibit A); *see also In re Application of the U.S.A. for an Order Authorizing the Use of a Pen Register and Trap on Internet Service Account/User Name*, 396 F.Supp.2d 45, 49 (D. Mass 2005) ("contents" included URL "subject lines, application commands, search queries, requested files names, and *file paths*." *Id*. at 49-50 (emphasis added)); *U.S. v. Forrester*, 512 F.3d 500, n. 6 (9th Cir. 2008) (URL, unlike IP address, "reveals much more information" about user's Internet activity, including articles viewed). For example, consider the URL http://www.nick.com/videos/clip/digital-short-penguins-of-madagascar-shorts-skippers-nightmare.html.[20] Broken down, this URL contains the following parts:

1. ***http***://www.nick.com/videos/clip/digital-short-penguins-of-madagascar-shorts-skippers-nightmare.html.

[20] This URL is used only as an example to counter Viacom's contention that the sample URL used in the Complaint does not identify a specific video and therefore contains no "content". Viacom Motion to Dismiss at 8, 29. Viacom goes so far as to claim that "contents" only applies to the video and that Plaintiffs' claims fail because the sample URL provided in the Complaint does not identify a specific video. Plaintiffs could just have easily used the above URL, http://www.nick.com/videos/clip/digital-short-penguins-of-madagascar-shorts-skippers-nightmare.html, which links directly to a specific video and the title of that video plainly appears in the URL that would be transmitted to Defendants' through their respective cookies.

This part of the URL identifies the computer *language* (http:) the web-browser and host web-server will use to communicate.

2. **http**://***www.nick.com/***videos/clip/digital-short-penguins-of-madagascar-shorts-skippers-nightmare.html.

This part of the URL identifies the *name of the website* and the corresponding host web-server with which this person intended to communicate.

3. http://www.nick.com/***videos/clip/***digital-short-penguins-of-madagascar-shorts-skippers-nightmare.html.

This part of the URL identifies the *specific electronic folder(s)* on the host webserver that contain the contents of the information (in this case a video) the Internet user has requested.

4. ***http://www.nick.com/videos/clip/digital-short-penguins-of-madagascar-shorts-skippers-nightmare***.html.

This part of the URL identifies the *precise file, document, or in this case video,* contained within the folder the Internet user has requested.

5. http://www.nick.com/***videos/clip/digital-short-penguins-of-madagascar-shorts-skippers-nightmare***.html.

This combination of the folder and the precise file name is called the "*file path*."

This example shows how URLs contain significant substance, purport and meaning of user's communications with websites – here, a request from the user to view a specific video entitled, "Skipper's Nightmare" on Defendant Viacom's website.

Courts have carefully examined whether URL file paths constitute content and have rightly concluded that they do. For instance, in the *FISC Opinion* (attached as Exhibit A), the National Security Agency (NSA) sought permission to track URLs under the Pen Register Act.

Declassified portions of the opinion reveal that the NSA claimed that URLs were not "contents" because they are dialing, routing, addressing and signaling information (DRAS), and thus, mutually exclusive of "content." *Id*. at 30-31.

The FISC, which routinely deals with the ECPA, rejected this interpretation. "The breadth of the terms used by Congress to identify categories of information subject to collection and to define "contents" reinforces the conclusion that DRAS and contents are not mutually exclusive categories." *Id.* at 31-33 (noting " [A] URL can also include "contents" as defined in section 2510(8)") (citing *In re Application of the U.S.A.*, 396 F.Supp.2d at 49; *Pharmatrak*, 329 F.3d at 18 (URLs including search terms are "contents" under Section 2510(8)) (emphasis added). Yet, in some circumstances a URL can also include "contents" as defined in section 2510(8). *Id.* at 31.

Other examples illustrate how full-string URLs, which contain application commands, requested file names, file paths, and search queries, contain information "about the substance, purport or meaning" of the communications. URL file paths can simultaneously identify web locations and detail with great specificity the substance, purport and meaning, the "contents", of the Internet user's communication with the website. "The 'substance' and 'meaning' of the communication is that the user is conducting a search for information on a particular topic." *In re Application of the U.S.A.*, 396 F.Supp.2d at 49 (concluding "if the user then enters a search phrase, that search phrase would appear in the URL after the first forward slash. This would reveal content – that is it would reveal, in the words of the statute . . .'information concerning the substance, purport or meaning of that communication.'"). Indeed, anyone acquiring this URL and associating it with the person who performed the search can glean the precise substance of

that person's communication with Nick.com, and anyone following the URL can access the exact contents of the document the web server transmitted back to this person.[21]

Put in a traditional wiretap context, if this person had called Nickelodeon on the phone and requested the same video, and if Google had tapped that phone line and intercepted that request, there is no question such a communication would have included content, and that such conduct would violate the ECPA. Plaintiffs' allegations about Internet requests must be viewed no differently. *See also, In re Application of the U.S.A.*, 396 F.Supp.2d at 49 ("contents" included URL "subject lines, application commands, search queries, requested file names, and *file paths*."). *Id*. at 49-50 (emphasis added)); *Forrester*, 512 F.3d at 510, n. 6 (URL, unlike IP address, "reveals much more information" about user's Internet activity, including articles viewed); P.L. 107-56, PATRIOT Act, House Report No. 107-236(I) at 54 ("an order could not be used to collect information . . . *such as the portion of a URL (Uniform Resource Locator) specifying Web search terms or the name of a requested file or article")* (emphasis added). Either way, an interception of a substantive communication has occurred. The only difference is the technology used to accomplish that interception.

Google alleges that it would receive a copy of a URL even without having placed tracking cookies. Google Motion to Dismiss at 18. This assertion misses the point. Without its secretly implanted tracking cookie, Google would still receive URLs in the form of GET requests executed at the request of the web site host server. But without the cookie and its unique

[21] Federal courts have also held that mere numbers can be considered "contents" as well. *See Brown v. Waddell*, 50 F.3d 285, 87-88 (4th Cir. 1995) (Numbers sent to a pager which are "more extensive … than those in telephone numbers" contain "contents.") and *U.S. Telecom Assoc. v. FCC*, 227 F.3d 450 (D.C. 2000) ("Post-cut-through digits" entered by a telephone caller after being connected to the recipient of their call "can also represent call content.") If mere numbers punched into a telephone can constitute content, so too must words that detail an Internet user's precise communications with the websites with which he or she chooses to interact.

persistent identifier, that URL could not be associated with any specific child's online communications. That is why numerous authorities recognize that the interception of URLs tied to the identity of a particular Internet user is the interception of content. *In re Application of the U.S.A.*, 396 F.Supp. at 49; *Forrester*, 512 F.3d 500, n. 6; *Pharmatrak*, 329 F.3d at 18-22; *see also FISC Opinion* at 32-33 (noting concepts of "content" and "non-content" are not mutually exclusive so URLs can be both, depending on function).

b. Birthdate and Gender Are Also "Contents" Under the ECPA

Plaintiffs also allege that Defendants' cookies intercepted personal information from Plaintiffs such as their gender and birthdate. (Complaint ¶81-82). Defendants' Motions noticeably fail to make any argument regarding whether birthdate and gender qualify as contents under the ECPA. Such information clearly falls under the ECPA definition of contents since they convey "information concerning the substance, purport, or meaning" of minor Plaintiffs in this action.

In *Yunker v. Pandora Media, Inc.*, the Northern District of California confronted this precise question. *Yunker v. Pandora Media, Inc.*, No. 11-CV-03113, 2013 WL 1282980, at *6 (N.D. Cal. March 26, 2013). After analyzing several cases on point, the court in *Yunker* drew an important distinction between: (1) information generated automatically by a web browser or cell phone due to their respective programming; and (2) personal information, like birthdate and gender, sent after being entered by a user. *Id*. at *6-7.

Here, just as in *Yunker*, Plaintiffs entered sensitive personal information which was hijacked by Defendants' cookies and conveyed without Plaintiffs' consent. Information like gender and birthday are undeniably content under the ECPA. At the barest minimum, these allegations present a factual question for discovery.

3. Defendant Viacom Can Be Liable Under the ECPA for Defendant Google's Conduct

Plaintiffs' Complaint seeks in part to impose liability on Viacom for Google's placement of third party cookies on Viacom's websites. (Complaint ¶¶ 73-74). Viacom alleges that this type of secondary liability is impermissible. Viacom Motion to Dismiss at 30-31. Defendants are incorrect as Viacom can be held liable for procuring Google to violate the ECPA. After all, Google would not have been able to place their cookies on Viacom's websites without Viacom's knowledge and consent.

Specifically, Viacom relies on the language of § 2520 and how it was altered from its original form to the amended statute currently in effect. The original statute read as follows:

> Any person whose wire or oral communication is intercepted . . . in violation of this chapter shall (1) have a civil cause of action against any person who intercepts ... or procures any other person to intercept . . . such communications, and (2) be entitled to recover from any such person [damages, attorney's fees and costs].

18 U.S.C. § 2520 (1982). The amended statute now reads:

> [A]ny person whose wire, oral, or electronic communication is intercepted . . . in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

18 U.S.C. § 2520 (2000).

Viacom contends that the absence of the word "procures" in the new statute prohibits Plaintiffs from holding Viacom liable for Google's violations of the ECPA. This is not the case. *See Lonegan v. Hasty*, 436 F.Supp.2d 419, 428 (E.D. N.Y. 2006) (holding procurement liability still exists under the ECPA). The court in *Lonegan* resolved this issue by noting that:

> [T]he more natural reading of the amended statute shows no intent on the part of Congress to eliminate the private right of action for procurement violations. . . Pursuant to Section 2511(1)(a) . . . violation of the Wiretap Act includes those

> persons whose communications are intercepted by someone who was procured to do so by a third party.

Id. The *Lonegan* court conducted a thorough analysis of the legislative history and concluded that "Congress intended to streamline the language of the provision . . . but that it did not, in so doing, intend to eliminate procurement violations from civil liability." *Id*. Thus, Plaintiffs may maintain a cause of action against Viacom for procuring Google to violate Plaintiffs' rights under the ECPA.

4. Defendants Fail to Address Plaintiffs' Wiretap Claims Against Google for Tracking Plaintiffs' on Non-Viacom Websites

In addition to alleging the Defendants violated the Wiretap Act by tracking the content of the Plaintiffs' communications on Viacom's websites, Plaintiffs have also alleged an ECPA claim based on Google's interception of "Plaintiffs' communications with other websites on which Google places advertisements and related tracking cookies despite Google's knowledge that the Plaintiffs were minor children and without … consent." (Complaint ¶155). Google neither mentions nor challenges this claim. Google's conduct, accepted as true, provides a separate and unchallenged basis for liability under the ECPA.

E. PLAINTIFFS' STATE LAW CLAIMS ARE NOT PREEMPTED BY THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT

Viacom argues Plaintiffs' state law claims are expressly preempted by the Children's Online Privacy Protection Act ("COPPA"). Viacom Motion to Dismiss at 32-34. Federal law preempts state law where: (1) the federal statute expressly says so ("express preemption"); (2) Congress preempts the entire field of law ("field preemption"); or, (3) the state and federal laws require conflicting or inconsistent compliance ("conflict preemption"). *See Arizona v. U.S.*, 132 S. Ct. 2492, 2500-01 (2012). Viacom relies solely on express preemption. Viacom Motion to Dismiss at 33. That is, Viacom has not asserted field or conflict preemption. *Id*.

In summary form, COPPA requires an "operator of any website or online service" to obtain parental consent before it collects or uses the "personal information" of a "child," where the child is "under the age of 13." *See, e.g.*, 15 U.S.C. §§ 6501(1), 6502(a), 6502(b)(1)(A)(ii); 16 CFR part 312. Section 6502(d) of the Act provides that "[n]o State or local government may impose any liability for . . . activities or actions by operators . . . in connection with an activity or action described in this chapter *that is inconsistent with* the treatment of those activities or actions under this section." *Id*. § 6502(d) (emphasis added). In conclusory fashion, Viacom argues Plaintiffs' state-law claims "would seek to impose liability for conduct that would be 'inconsistent' with COPPA's treatment of such activities." Viacom Motion to Dismiss 33. Thus, Viacom impermissibly extrapolates that the statute, which Congress believed necessary to provide a safer, more secure online experience for children, expressly preempts all state-law claims brought by those same children whose privacy rights were violated by website/online-service operators. *Id. (citing Cohen v. Facebook* (California Superior Court, County of Los Angeles Case No. BC44482, (July 5, 2011)), Appended to Viacom's Motion to Dismiss.

As an initial matter, *Cohen* does not support Viacom's preemption argument. Contrary to Viacom's representation, *Cohen* did not find all "'minors' state-law right of publicity and other claims arising out of online activity were preempted by COPPA." Viacom Motion to Dismiss 33-34. Indeed, the court's order was specifically limited to "Plaintiffs' claims based on state law for Facebook's alleged failure to obtain the parental consent of users *aged 13 to 17*." Viacom Appendix to Motion to Dismiss, Ex. A (9/22/11 Minute Entry) and Ex. B at pp. 2-3 (9/22/11 Hearing Transcript) (emphasis added). Because COPPA applies only where the child is "under the age of 13," the *Cohen* court concluded preemption under COPPA barred efforts by the

plaintiffs to use state law to impose a parental consent requirement for minors *aged 13 to 17*.[22] But, the court did not find (or apparently even consider) preemption of the state-law privacy claims asserted by users under 13. Viacom Appendix to Motion to Dismiss, Ex. B at p. 3. Unlike *Cohen*, the proposed class in this case includes children under 13. *Cohen* is thus inapposite and does not support dismissal of Plaintiffs' state-law claims.

Viacom's argument fares no better under traditional preemption principals. While COPPA includes an express-preemption provision, at least with respect to "inconsistent" state law (15 U.S.C. § 6502(d)), the existence of such a provision, alone, does not end the inquiry. *See, Farina v. Nokia, Inc.*, 625 F.3d 97, 118 (3d Cir. 2010), *cert. denied*, 132 S. Ct. 365 (2011) (confirming "the presence of an express preemption provision does not end the inquiry"); *Medtronic, Inc. v. Lohr*, 518 U.S. 470, 484-85 (1996) (same). While courts need not inquire whether Congress intended to preempt *some* state law, courts still must examine congressional intent as to the scope of the preemption provision. *See, Lohr*, 518 U.S. at 485–86. Thus, the task is to identify the domain expressly preempted, because "an express definition of the pre-emptive reach of a statute ... supports a reasonable inference ... that Congress did not intend to preempt other matters," *See Freightliner Corp. v. Myrick*, 514 U.S. 280, 288 (1995); *Cipollone v. Liggett Group, Inc*., 505 U.S. 504, 517 (1992).

The Court's analysis must be guided by two cornerstones of preemption jurisprudence. *Wyeth v. Levine*, 555 U.S. 555, 565 (2009); *see also, Farina*, 625 F.3d at 115. First, "the purpose of Congress is the ultimate touchstone in every preemption case." *Lohr*, 518 U.S. at 485.

[22] Congress initially considered a requirement that operators make reasonable efforts to provide parents with notice and an opportunity to prevent or curtail the collection or use of personal information collected from children over the age of 12 and under the age of 17. *See* Children's Online Privacy Protection Act of 1998, S. 2326, 105th Cong. § 3(a)(2)(iii) (1998). Ultimately, however, Congress decided to define a child as an individual under age 13. 15 U.S.C. § 6501(1).

Second, "[i]n all preemption cases, and particularly in those in which Congress has 'legislated ... in a field which the States have traditionally occupied,' ... [courts] 'start with the assumption that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress.'" *Id*. (quoting *Rice v. Santa Fe Elevator Corp*., 331 U.S. 218, 230 (1947)). "[B]ecause the States are independent sovereigns in our federal system, [courts] have long presumed that Congress does not cavalierly preempt state-law causes of action." *Lohr*, 518 U.S. at 485. That is, there is a "presumption *against* preemption," *Wyeth*, 555 U.S. at 555 n. 3 (emphasis added), which applies with particular force in fields within the police power of the state. *See, Lohr*, 518 U.S. at 475, 485.

It is beyond dispute that the protection of privacy rights traditionally falls within the police power of the state. While Congress has, over the last few decades, enacted various federal privacy-related statutes, the responsibility for citizens' well-being has been traditionally vested in the States. *See, id*. (confirming "States traditionally have had great latitude under their police powers to legislate as to the protection of the lives, limbs, health, comfort, and quiet of all persons."). Thus, this Court's analysis starts with a presumption that Congress did not preempt all state-law claims in the enactment of COPPA.

The issue, then, is whether Viacom has overcome that presumption by demonstrating a clear Congressional purpose to preempt or that the existence of a conflict between state and federal law is "clear and manifest." *See Farina*, 625 F.3d at 117, citing *Fellner v. TriUnion Seafoods LLC*, 539 F.3d 237, 249 (3rd Cir. 2008), *cert. denied*, 129 S. Ct. 1987 (2009). Viacom has shown neither. Indeed, Viacom's entire analysis consists of citing the statute and then summarily concluding Plaintiffs' state-law claims "seek to impose liability for conduct that would be 'inconsistent' with COPPA." Viacom Motion to Dismiss 33.

Regardless, however, an examination of the basic purpose of the legislation supports the conclusion that COPPA does not preempt all state law claims. The Act was developed to prohibit unfair and deceptive acts and practices in connection with the collection and use of personally-identifiable information from and about children on the internet. The goals were to enhance parental involvement in a child's activities online, protect the safety of a child while participating in online locations such as chat rooms, secure a child's personally identifiable information collected online, and limit information collection from a child absent parental consent.[23]

To effectuate those goals, Congress included five key requirements: (1) notice, (2) parental consent, (3) parental review, (4) limitations on the use of games and prizes, and (5) security. 15 U.S.C. §§ 6502(b)(1)(A-D); *see also* 16 CFR §§ 312.4(b)-312.8. And, while Congress included a limited preemption provision, the purpose of that provision was not to preclude all state regulation of children's online privacy, but instead to prevent state and local governments from adopting requirements that are inconsistent with those imposed by COPPA. 15 U.S.C. § 6502(d).

Here, Plaintiffs' state law claims do not seek to impose liability for activities that are inconsistent with those set forth in the COPPA. To the contrary, Plaintiffs state law privacy claims are based primarily on Viacom's collection and use of personal information without parental consent.[24] Those claims, of course, are *entirely consistent* with COPPA's mandate that

[23] Notice of Proposed Rulemaking and Request for Public Comment, 64 FR 22750 (Apr. 27, 1999), citing 144 Cong. Rec. S12741 (daily ed. Oct. 7, 1998) (Statement of Sen. Bryan)).

[24] For example, Plaintiffs' claims common law tort claim—intrusion upon seclusion—is premised on Viacom's failure to obtain consent before tracking Plaintiffs' on the internet, which is consistent with COPPA's parental consent requirement. *See* Complaint ¶¶ 194-197. Plaintiffs' claims under the California Invasion of Privacy Act are likewise premised on the failure to obtain the consent of Plaintiffs or their parents to track their personal communications.

operators of websites/online services obtain parental consent for the collection, use or disclosure of personal information from children. 15 U.S.C. S. 6502(b)(1)(A)(ii). Thus, Plaintiffs' state law claims are not "inconsistent with" the activities covered by the COPPA.

Simply put, COPPA was not intended to preempt state law claims based on duties that are consistent with the Act. Thus, the Act preempts only those state laws that are "inconsistent" with "an activity or action described in [COPPA]." 15 U.S.C. § 6502(d). As drafted, section 6502(d) signifies that Congress did not intend to preempt all state law. Consequently, Viacom's motion to dismiss Plaintiffs' state law claims, to the extent it is premised on preemption grounds, should be denied.

F. PLAINTIFFS PROPERLY PLED A CALIFORNIA INVASION OF PRIVACY ACT CLAIM

The California Invasion of Privacy Act ("CIPA") prohibits any person who "willfully and without the consent of *all* parties to the communication, or in any unauthorized manner" attempts to read or learn the "the contents or meaning of any message, report or communication while the same is in transit . . . ." Cal. Penal Code § 631(a) (emphasis added).[25] CIPA's "all consent" statute is more stringent than the Federal Wiretap Act, which only requires "one of the parties to the communication" to consent to interception. 18 U.S.C. § 2511(d).

Defendants' recycled Wiretap Act claim arguments fail under CIPA as well. Defendant Google first claims that it was a party to the communication. Google Motion to Dismiss at 24. Not so. *See In re Google Inc. Cookie Placement Consumer Privacy Litig.* ("*Google Cookie*

See id. ¶¶ 175-187. And Plaintiffs' claims under the New Jersey Computed Related Offenses Act are similarly premised on the actions taken by Viacom without consent. *Id*. ¶¶ 188-193.

[25] Defendant Viacom attempts to skirt Section 631(a) by claiming the statue does not provide a right of action for those who merely aid and abet violators. (Viacom Motion to Dismiss at 34, *citing* Cal. Penal Code § 637.2 [actions permitted "against the person who committed the violation . . . ."]). Here, Defendant Viacom "permitted, acquiesced to, facilitated, *and participated*" in activity which violated Section 631(a). (Complaint ¶ 184) (emphasis added). In so doing, Defendant Viacom violated the California Penal Code and is properly subject to suit.

Litigation"), No. 12-2358-SLR, 2013 WL 5582866, at *4 (D. Del., Oct. 9, 2013) ("Google is not appropriately deemed a party to the communications.") Moreover, Google still violated CIPA even if it was a party to the communication because it failed to obtain "the consent of *all* parties to the communication" when placing and/or accessing cookies on Plaintiffs' computers. Cal. Penal Code § 631(a) (emphasis added); (Complaint ¶¶ 102, 137, 144, 150-51, 177, 182-83).

Both Defendants claim that no protected communication was intercepted. (Google Motion to Dismiss at 24; Viacom Motion to Dismiss at 34) (*citing Google Cookie Litig.*, 2013 WL 5582866 at *5). While the *Google Cookie Litigation* court correctly stated that "Google would have received the inputted information, including the URL, regardless of the setting of third-party cookies," it failed to acknowledge that this information takes on new meaning when it is matched up with an individual child via a cookie's unique identifier. *Id*. at **5-6. Rather than receiving anonymous bits of information about users, Google uses the cookie to track the user's activity, build a profile, and, as that court admitted, "send different information in response to targeted advertising than would have been sent without the setting of third-party cookies." *Id*. at *4. This combination – cookies plus URL and other information – constitutes a communication with content, protected under CIPA. *Id*. at *5.

Nor does the federal Wiretap Act preempt Plaintiffs' CIPA claim as Defendant Google contends. (Google Br. at 23-24 n. 8). As the California Supreme Court made manifest in *Kearney v. Salomon Smith Barney, Inc.*, the Wiretap Act's legislative history reveals a Congressional intent that "[s]tates would be free to adopt *more restrictive* legislation, or no legislation, but not less restrictive legislation." *Kearney v. Salomon Smith Barney, Inc.*, 39 Cal.4th 95, 105 (2006) (emphasis in original) (quoting *People v. Conklin*, 12 Cal.3d 259, 270–273 (1974)); *see also Leong v. Carrier IQ Inc*, No. 12-01562, 2012 WL 1463313, at *5 (C.D.

Cal. April 27, 2012) (finding against preemption); *accord Valentine v. NebuAd, Inc.*, 804 F.Supp.2d 1022, 1029 (N.D. Cal. 2011). Indeed, the court in *Shively v. Carrier IQ, Inc.* was persuaded by *Leong* and *Valentine* but rejected cases Defendant Google cites[26] because "the latter cases do not address the legislative history . . . and because complete preemption is a rarity that arises only in extraordinary situations." *Shively v. Carrier IQ, Inc.*, No. 12-md-2330, 2012 WL 3026553, at **8, 10 (N.D. Cal. July 24, 2012) (finding no express or implied preemption).

G. PLAINTIFFS PROPERLY PLED A STORED COMMUNICATIONS ACT CLAIM

The Stored Communications Act (SCA) provides a cause of action against "whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided, or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system . . . ." 18 U.S.C. § 2701(a).

1. Plaintiffs Properly Identify Communications in Electronic Storage Under the SCA

A violation of the SCA is premised upon the improper access of an electronic communication in "storage." 18 U.S.C. § 2701(a)(2). The ECPA, of which the SCA is a part, defines "electronic storage" as "(a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

Google claims that Plaintiffs' SCA claim is incompatible with Plaintiffs' Wiretap claim, which requires improper "interception" of an electronic communication in transit. 18 U.S.C.A.

[26] Defendant Google cites, *inter alia*, *Bunnell v. Motion Picture Ass'n of Am.*, 567 F. Supp. 2d 1148 (C.D. Cal. 2007) and *In re Google Inc. St. View Elec. Commc'n Litig.*, 794 F. Supp. 2d 1067. (N.D. Cal. 2011).

§§ 2510; 2511(1); (*see* Google Motion to Dismiss at 25) ("Because communications cannot simultaneously be 'in transit' and 'in storage,' Plaintiffs' SCA claim fails.").

Again, Google misses the mark. Electronic communications on the Internet are broken up into constituent packets of information that make multiple stops "from router to router within a network to find a path toward the ultimate destination." *U.S. v. Szymuszkiewicz*, 622 F.3d 701, 704 (7th Cir. 2010) (finding it irrelevant, for the purposes of a Wiretap Act claim, whether an email communication was improperly accessed "in flight" at the server, or after it was delivered to the intended computer). Thus, "technology has, to some extent, overtaken language. Traveling the Internet, electronic communications are often--perhaps constantly--both "in transit" and "in storage" simultaneously, a linguistic but not a technological paradox." *See U.S. v. Councilman*, 245 F.Supp.2d 319, 321 (D. Mass. 2003) (nevertheless dismissing plaintiff's Wiretap Act claim, because in-transit email communications were briefly housed in random access memory ('RAM') storage when accessed, and were therefore not "intercepted.").

Following the District Court ruling in *Councilman*, the First Circuit Court of Appeals, *en banc*, subsequently vacated and remanded. *U.S. v. Councilman*, 418 F.3d 67 (1st Cir. 2005). The First Circuit held that the emails at issue, which were accessed while temporarily in electronic storage while en route to their destination, were "intercepted" electronic communications for purposes of the Wiretap Act. *Id.* at 79. The court likewise acknowledged that accessing such emails in temporary electronic storage could also violate the SCA. *Id.* at 81-82 ("In general, if two statutes cover the same conduct, the government may charge a violation of either."); *see also Szymuszkiewicz*, 622 F.3d at 705 (finding that both the Wiretap Act and the SCA are each "fully enforceable according to [their] own terms").

Here, it is likewise consistent to claim that these communications were improperly accessed both while in transit per the Wiretap Act, and while in electronic storage per the SCA. Defendant Google placed and/or accessed cookies on Plaintiffs' computers between the time the child sent a "GET" command to the Nick.com server and the time all of the content was sent back to the child's browser for display. (Complaint ¶ 24-31, 39-46). This entire process occurred within milliseconds. (Complaint ¶ 46). Thereafter, using its cookies, Defendant Google intercepted Plaintiffs' web communications whenever Plaintiffs' web browsers issued "GET" commands to travel the internet and visit websites where Defendant displayed advertisements. (Complaint ¶¶ 39-47, 72-77). To place and/or access its cookies to monitor such communications, however, Defendant Google had to access the browser managed files within Plaintiffs' computers, where cookies are housed. (Complaint ¶¶ 161-174). Both claims are factually consistent, properly pled, and this motion should be denied.

2. Plaintiffs Properly Identify a Facility Under the SCA

Under the SCA, a "facility" can be anything "through which an electronic communication service is provided." 18 U.S.C. § 2701(a); *see Cousineau v. Microsoft Corp.*, No. C11-143B-JCC, 2012 WL 10182645, at *6 (W.D. Wash. June 22, 2012) ("Congress chose a broad term—facility—because it intended the statute "to cover a particular *function, such as internet access, as opposed to a particular piece of equipment* providing that access . . . .") (emphasis added).

This definition includes facilities operated by third party Electronic Communication Service ("ECS") providers, such as internet service providers ("ISPs"), email servers, and electronic bulletin boards. *See Chance v. Avenue A, Inc.*, 165 F.Supp.2d 1153, 1160 (W.D. Wash. 2001). Yet, by the plain language of the statute, the broad term "facility" also includes

personal devices and software that serve as a conduit for third party provided ECS. 18 U.S.C. § 2701(a); *see, e.g., Cousineau,* 2012 WL 10182645 at *6 (finding plaintiffs' mobile device could be a facility for the purposes of the SCA).

As such, the "facility" analysis is two-fold. First, there must an ECS provided; and, second there must be something (the facility) through which that service is provided. 18 U.S.C. § 2701(a).

a. Plaintiffs' Internet Service Providers and Web Browsers Provide Electronic Communications Services as Defined in 18 U.S.C. § 2510(15)

The ECPA defines "electronic communication service" broadly to include "*any* service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (emphasis added). Both ISPs, like Comcast, and web browsers, like Google Chrome and Apple Safari, satisfy this definition. (Complaint ¶¶ 24,166-167). ISPs are physical infrastructure that help fulfill web browsers' requests. In turn, web browsers provide a service Internet users employ to send and receive electronic communications over the Internet.[27] 18 U.S.C. § 2510(15).

b. Plaintiffs' Computers and the Browser Managed Files Within Them That Store Information are "Facilities"

In light of the plain language of 18 U.S.C. 2701(a), anything that acts as a "conduit" for ECS qualifies as a "facility" for purposes of the SCA. *See, Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 902 (9th Cir. 2008) (noting that electronic communications pass through a "conduit") (reversed on other grounds by *City of Ontario, Cal. v. Quon,* 560 U.S. 746 (2010)).

[27] *See* http://googleblog.blogspot.com/2008/09/fresh-take-on-browser.html (last visited February 4, 2014) ("We search, chat, email and collaborate in a browser. And in our spare time, we shop, bank, read news and keep in touch with friends -- all using a browser.").

Here, both Plaintiffs' computers and the browser managed files contained within them[28] are "facilities" because they act as the "conduit" through which ISPs and browsers provide ECS. *See, Chance*, 165 F.Supp.2d at 1161 ("[v]iewing this *factual* dispute in the light most favorable to the non-movant, as is required on summary judgment, it is possible to conclude that modern computers, which serve as a conduit for the web server's communication to [defendant], are facilities covered under the act.") (emphasis added); *Expert Janitorial, LLC v. Williams*, No. 3:09-CV-283, 2010 WL 908740 at *5 (E.D. Tenn. 2010) ("it appears to the Court that plaintiff's computers on which the data was stored may constitute 'facilities' under the SCA") (citing *Becker v. Toca*, No. 07-7202, 2008 WL 4443050 at * 4 (E.D. La. 2008)).

Defendant Google's claim that "Plaintiffs' interpretation would 'render other parts of the statute illogical'" is based on faulty reasoning. (Google Motion to Dismiss at 26) (*citing In re iPhone Application Litig*. ("*iPhone II*"), 844 F. Supp. 2d 1040, 1058 (N.D. Cal. 2012). The court in *iPhone II* relied on two statutory exceptions to reject the notion that a personal computer could be a "facility" under the SCA. *Id*. Specifically, Section 2701(c)(1) provides that the SCA's prohibitions against accessing stored information do not apply to conduct authorized by *providers* of ECS, and Section 2701(c)(2) provides that such prohibitions do not apply to conduct authorized by *users* of ECS. If a personal computer is classified as a *facility providing ECS*, as the court in *iPhone II* reasoned, then Section 2701(c)'s statutory distinctions would indeed be rendered meaningless: users would become providers and vice versa, allowing for all types of access and disclosure not contemplated by the SCA. *Id*. at 1058. Google parrots *iPhone*

[28] Web browsers store cookie and other information via browser-managed files on personal computing devices. (Complaint ¶ 169).

II's rationale, which was also adopted wholesale by the court in *Google Cookie Litig*., 2013 WL 5582866 at *7.[29]

Yet this analysis conflates the concept of a "facility" and an "electronic communication service" provider. For example, the *iPhone II* court emphasized that "courts that have taken a closer look have consistently concluded that an individual's personal computer does not 'provide an electronic communication service' simply by virtue of enabling use of electronic communication services." *iPhone II*, 844 F.Supp.2d at 1058. Contrary to the plain language of the statute, this analysis assumes that the "facility" must also be the provider of ECS. 18 U.S.C. § 2701(a).

Plaintiffs do not contend that their personal computers, or the browser managed files on those computers, are the providers of the ECS at issue. (Complaint ¶¶ 169. 171-172). Instead, as "facilities," they are merely the conduit for ECS provided by third party ISPs and web browsers. (Complaint ¶¶ 166-167) (identifying ISPs and web browsers as providers of ECS). In other words, Plaintiffs' personal computers and browser managed files are the thing "*through which* an electronic communication service is provided." 18 U.S.C. § 2701(a) (emphasis added); *see In re Intuit Privacy Litig.*, 138 F.Supp.2d 1272, 1282 n. 3 (C.D. Cal. 2001) (the SCA "does not require that Plaintiffs' computers to be 'communication service providers' only that they be a facility through which an electronic communication service is provided."); *accord Expert Janitorial, LLC*, 2010 WL 908740 at *5 (finding "that plaintiff's computers on which the data was stored may constitute 'facilities' under the SCA."

[29] For example, the *Google Cookie Litig.* court concluded that classifying a personal computer as a "facility" would be inconsistent with § 1701(c)(2) in that it would make the web site the "user" of a communication service provided by an individual's computer such that any communication between the individual's computer and the website would be a communication intended for that website, thus, triggering the § 2701(c)(2) exception for authorized access. *Google Cookie Litig.*, 2013 WL 5582866 at *7 (citing *In re iPhone II*., 844 F.Supp.2d at 1058).

Moreover, neither Section 2701(c)(1) nor 2701(c)(2) are rendered nonsensical by recognizing that a personal computer can qualify as a facility through which ECS is provided by a third party. Although an ECS provider may authorize disclosure under 2701(c)(1), the circumstances under which such disclosures may take place are exhaustively outlined in Section 2702(b)(c). These provisions must be construed together to give effect to the Act as a whole. *See, e.g., F.D.A. v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 132 (2000) (finding that, where possible, courts must fit all parts of a statute into a harmonious whole). Thus, Google's claim that construing personal computers as "facilities" would allow ECS providers unrestricted authority to share user's communications is unwarranted. Google Motion to Dismiss at 26.

Further, the Plaintiffs remain the "users" of ECS for purposes of the Section 2701(c)(2) statutory exception analysis. This is because Plaintiffs' computers are merely "facilities" providing a conduit through which ISPs and web browsers provide them with ECS. As a result, the fear that "embracing this expanded notion of the term 'facility' [will] confound[] the distinction between 'users' and 'providers' . . . ." is likewise unwarranted. *Google Cookie Litig.*, 2013 WL 5582866 at *7.

3. Plaintiffs Have Shown That Defendant Google's Access Was Unauthorized

Plaintiffs in this action constitute a class of "children under the age of 13 in the United States . . . ." (Complaint ¶¶ 1-3; 9-15). As such, Plaintiffs could not legally authorize Defendant Google to place or access cookies on Plaintiffs' computers. Indeed, to protect children, "[t]he law properly may subject minors to more stringent limitations . . . ." *Planned Parenthood of Central Mo. v. Danforth Eyeglasses*, 428 U.S. 52, 72 (1976) (listing examples: appointing a guardian ad litem for a court proceeding, prohibiting the sale of firearms to minors without parental consent, etc.). Yet here, Google did not receive consent from either Plaintiffs or their

guardians before monitoring the internet usage of minor children. (Complaint ¶¶ 102, 137, 144, 150, 151, 177, 182-83). As such, Google's conduct was unauthorized.

Without addressing Plaintiffs' inability to consent to its conduct, Google instead makes a passing assertion that Plaintiffs' SCA claim fails under *DoubleClick*, 154 F. Supp. 2d at 507, 513-14. Google Motion to Dismiss at 27.[30] There, the court dismissed an SCA claim because defendant DoubleClick fell within Section 2701(c)(2), which provides a statutory exception for conduct authorized by "a user of that service with respect to a communication of or intended for that user . . . ." 18 U.S.C. § 2701(c)(2). The *DoubleClick* court rationalized that since "cookies' identification numbers are internal DoubleClick communications -- both 'of' and 'intended for' DoubleClick," -- access was authorized and "it does not violate Title II for DoubleClick to obtain them from plaintiffs' electronic storage." *Id*. at 513.

Yet this analysis assumes that DoubleClick (and, here, Google) are "users" of an electronic communication service under Section 2701(c), a notion that the *Google Cookie Litig.* Court flatly rejected: "With respect to the legislative history of the SCA … , there can be no dispute that the individual owners of personal computers were the 'users' contemplated under the statute and that the 'providers' of the 'electronic communication services' were contemplated to be third parties." *Google Cookie Litig.*, 2013 WL 5582866 at *7. The users at issue here are minor children using personal computers. They have not, and cannot, authorize Google's unlawful conduct. The conduct here was not authorized, and the SCA claim should be allowed to proceed.

[30] Although "courts may dismiss a claim based on a statutory exception that appears on the face of the complaint," here defendant does not so much as mention any specific statutory exception, much less point to any allegation appearing on the face of Plaintiffs' Complaint that establishes Google was authorized to access its cookies on Plaintiffs' computers. *See DoubleClick*, 154 F. Supp. 2d at 507, 513-14. Defendant's claim is thus insufficient to warrant dismissal.

H. PLAINTIFFS PROPERLY PLEAD CLAIMS UNDER THE NEW JERSEY COMPUTER RELATED OFFENSES ACT

Plaintiffs properly plead all necessary elements of a claim under the New Jersey Computer Related Offenses Act ("NJCROA") sufficient to survive Defendants' Motions to Dismiss. *See PNY Tech., Inc. v. Salhi*, No. 2:12-cv-04916, 2013 WL 4039030, at *6 (D.N.J. August 05, 2013) (holding plaintiff's NJCROA claim is sufficient to defeat Motion to Dismiss by stating defendant intentionally/knowingly altered data on plaintiff's computer without or in excess of authorization); *P.C. of Yonkers, Inc. v. Celebrations! The Party And Seasonal Superstore, L.L.C.*, No. 04-4554, 2007 WL 708978, at 9 (D.N.J. March 05, 2007) (same). The NJCROA provides that:

> A person . . . damaged in business or property as a result of any of the following actions may sue the actor therefor . . . and may recover compensatory and punitive damages and the cost of suit including a reasonable attorney's fee, costs of investigation and litigation:
>
> a. The purposeful or knowing, and unauthorized altering . . . of any data, database, computer program, computer software or computer equipment . . . ;
> b. The purposeful or knowing, and unauthorized altering . . . of a computer . . . ;
> c. The purposeful or knowing, and unauthorized accessing or attempts to access any computer . . . ;
> d. The purposeful or knowing, and unauthorized altering . . . of a financial instrument; or
> e. The purposeful or knowing accessing and reckless altering . . . of any . . . computer, computer program, computer software . . . .

N.J.S.A. 2A:38A-3. Google spends several pages of its Motion comparing a myriad of other statutes to the NJCROA. At one point, Google even goes so far as to allege that "[t]he term access is defined by section 2A:3A-1(a) [of the NJCROA] in terms redolent of hacking or breaking into a computer, which is different from the ordinary, everyday use of a computer." Google Br. at 36 (internal quotations removed). In support of its argument, Google cites *Chrisman v. City of Los Angeles*, a California case discussing California Penal Code Section 502.

Focusing on the statute at issue here, the NJCROA is clear on its face and requires no comparisons to penal codes from other states in order for this Court to understand and evaluate Plaintiffs' claims. *See Lozano v. Frank De Luca Constr.*, 178 N.J. 513, 522 (2004) ("We first look to the words of the statute, and if the language is clear, we interpret the statute consistent with its plain meaning.").

Here, Plaintiffs are all minor children under the age of 13 registered with Defendant Viacom's websites. (Complaint ¶4; *see also id*. at ¶¶ 9, 191, 192) (noting Plaintiffs' C.A.F., C.T.F., M.P. and T.P all reside in New Jersey). Plaintiffs were all damaged in property as a result of Defendants' cookies that: (1) altered their computers; (2) necessitated an investigation that took time and money to identify and remove the offensive cookie software; and (3) permitted the illegal acquisition and use of Plaintiffs' personal information for marketing purposes. (Complaint ¶¶ 49-59, 107, 190, 193); *see, Alston*, 585 F.3d at 763 ("the fact that plaintiffs' injury is non-monetary is not dispositive. A plaintiff need not demonstrate that he or she suffered actual monetary damages, because the actual or threatened injury required by Art. III may exist solely by virtue of statutes creating legal rights . . .") (internal citations and quotations omitted). Certainly, the parties will argue as to the actual monetary value of these damage claims, but the NJCROA specifically states that "[t]he value of damage, loss, property or income involved in any lawsuit shall be determined by the trier of fact." N.J.S.A. 2A:38A-4. Thus, it would be inappropriate for the Court to grant Defendants' Motions because there are matters to be settled by the trier of fact. *See*, *Marcus v. Rogers*, No. L-4477-08, 2012 WL 2428046 (N.J. App. Div. June 28, 2012) (denying defendant's motion and noting jury was free to accept or reject testimony regarding debatable damage to plaintiff in business or property under NJCROA); *Fairway Dodge, Inc. v. Decker Dodge, Inc*., No. L-10100-00, 2005 WL 4077532, at

¶11 (N.J. App. Div. June 12, 2006) (noting with approval trial judge's decision to permit NJCROA to be heard by jury for jury's ultimate decision regarding validity of damages claimed).

As set forth in the Complaint, in placing cookies on Plaintiffs' computers, Defendants' conduct was purposeful or knowing. (Complaint at ¶¶ 72-74). Defendants cannot make a claim that they did not knowingly and purposefully place their cookies on Plaintiffs' computers, as the software was designed to automatically install upon Plaintiffs' first visit to one of the websites at issue. Id.; (see also Google Motion to Dismiss at 36) ("The only data Google obtained *by placing cookies on Plaintiffs' browsers* . . . .") (emphasis added).

Defendants' actions in placing their cookies on Plaintiffs' computers was unauthorized as it lacked the consent of Plaintiffs. (Complaint at ¶¶ 5, 6, 76). Defendants argue that they had Plaintiffs' consent when they placed their cookies on Plaintiffs' computers, but their contention is undermined by two facts. First, the placement of Defendants' cookies occurred before Plaintiffs had an opportunity to consent. (Complaint at ¶ 76). Second, as Plaintiffs are all minors under the age of 13, their consent is voidable and the mere institution of this action works to assert their rescission to any consent. *See, J.D.B,* 131 S.Ct. at 2403-04 ("Like this Court's own generalizations, the legal disqualifications placed on children as a class— *e.g.*, limitations on their ability to alienate property, *enter a binding contract enforceable against them*, and marry without parental consent—exhibit the settled understanding that the differentiating characteristics of youth are universal.") (emphasis added); *Mechanics Fin. Co. v. Paolino, 29* N.J. Super. 449, 453 (N.J. App. Div.1954) (stating that "[i]t is generally true that an infant may avoid his contract."); *Boyce v. Doyle,* 113 N.J. Super. 240, 242 (1971) (holding institution of legal action on behalf of minor is sufficient to operate as a rescission of contract signed by

minor). Plaintiffs are minor children who, in the eyes of the law, are incapable of understanding and appreciating the alleged consent they granted to Defendants. This is precisely why it is a well settled tenet of the judicial system that minors cannot consent to a binding contract and that any contract they unwittingly enter is voidable at the minor's election.

Even if this Court determines that Plaintiffs' consent was valid, N.J.S.A. 2A:38A-3(e) does not require "unauthorized" access. Plaintiffs allege that Defendants' actions were at the very least reckless. Defendants knew or at least should have known that users of Viacom's websites aimed at children would likely lack the capacity to consent to any agreement to place cookies on their computers. In ignoring this fact, Defendants' actions were at a bare minimum reckless and at worst they were intentional in preying on unsuspecting and unsophisticated children.

Finally, Defendants do not even attempt to claim that the final element of the NJCROA -- that Defendants cookies were placed on Plaintiffs' computers thereby altering the computer -- has not been met. (Complaint at ¶ 72, 73). Accordingly, this Court should deny Defendants' Motions with respect to the NJCROA as Plaintiffs have not only met but surpassed their burden.

I. PLAINTIFFS' COUNTS VI AND VII SUFFICIENTLY STATE COMMON LAW CLAIMS OF INTRUSION UPON SECLUSION AND UNJUST ENRICHMENT

Plaintiffs have properly pled state common law tort claims of intrusion upon seclusion, and unjust enrichment. New Jersey law applies to these causes of action, and each is pled with the requisite particularity to withstand this motion.

1. New Jersey Law Applies To The Common Law Claims

"A federal court sitting in diversity determines the substantive law to be applied by looking to the choice of law rules of the forum state." *Williams v. BASF Catalysts LLC*, No. 11-

1754, 2012 WL 6204182, at *11 n.4 (D.N.J. Dec. 12, 2012) (*citing Klaxon Co. v. Stentor Elec. Mfg. Co.*, 313 U.S. 487, 496-97 (1941)).

New Jersey applies the Restatement's "most significant relationship" test to tort and breach of contract claims. *Agostino v. Quest Diagnostics Inc.*, 256 F.R.D. 437, 461 (D.N.J. 2009). When applying this test, "courts must first determine whether there is an actual conflict between the competing state laws." *Goodman v. Goldman, Sachs & Co.*, No. 10-1247, 2010 U.S. Dist. LEXIS 132593, *11 (D.N.J. Dec. 14, 2010). Where there is no actual conflict, the analysis ends and the court applies the law of the forum state. *Agostino*, 256 F.R.D. at 461 (*citing In re Ford Motor Co.*, 110 F.3d 954, 965 (3d Cir. 1997)).

Here, Defendants do not contend any conflict exists related to intrusion upon seclusion, and, in fact, admit the state laws "are consonant" (Google Motion to Dismiss. at 37, n.17) and subject to common analysis (Viacom Motion to Dismiss at 36). Likewise, Defendants do not suggest any substantial differences in the various state unjust enrichment laws, and New Jersey courts have repeatedly held there is no material conflict in unjust enrichment laws from state to state.[31] *See, e.g., Snyder v. Farnam Cos., Inc.*, 792 F. Supp. 2d 712, 723 (D.N.J. 2011) ("Numerous courts have held that unjust enrichment laws do not vary in any substantive manner from state to state. . . . Since no actual conflict exists, New Jersey law will be applied to all plaintiffs' unjust enrichment claims.") (*citing In re Mercedes-Benz Tele Aid Contract Litig.*, 257 F.R.D. 46, 58 (D.N.J. 2009) (finding that any differences under the laws of the various states are "not material and do not create actual conflict"); *Agostino*, 256 F.R.D. at 464 ("[T]here are no

[31] Even in states where Defendants contend unjust enrichment is not a cause of action, "courts have held that unjust enrichment is equivalent to restitution, and have allowed litigants to seek unjust enrichment as a remedy." *In re iPhone Application Litig.*, No.: 11-MD-02250-LHK, 2011 WL 4403963, at *45 (N.D. Cal. Sept. 20, 2011) (*citing Dinosaur Dev., Inc. v. White*, 216 Cal. App. 3d 1310 (Cal. App. Ct. 1989)).

actual conflicts among the laws of unjust enrichment"). Because there is no conflict between the competing state laws, New Jersey law applies to these claims.[32]

2. Plaintiffs State a Claim for Intrusion Upon Seclusion

New Jersey recognizes a cause of action for invasion of privacy by unreasonable intrusion upon seclusion, and follows the Second Restatement of Torts, which sets forth the elements as follows:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Castro v. NYT Television, 384 N.J. Super. 601, 608-09 (N.J. App. Div. 2006) (*quoting 3 Restatement (Second) of Torts* § 652B (1977)).

a. Defendants Intentionally Intruded Upon Plaintiffs' Seclusion and Private Affairs

Google argues that an intentional intrusion requires pleading that Defendant knew it was violating the law. (Google Motion to Dismiss at 38). However, intrusion upon seclusion does not "require a complainant to have knowledge of the reasons for the intrusion. Rather, the intentional intrusion itself . . . is sufficient to establish these torts." *Yates v. Commer. Index*

[32] If a conflict somehow does exist, the Court should "not conduct a choice of law analysis because it would be premature to do so at this point in the case, prior to the development of the factual record." *Williams*, 2012 WL 6204182 at *33 n.4 (*citing Harper v. LG Electronics USA, Inc*., 595 F. Supp. 2d 486, 491 (D.N.J. 2009) (declining to engage in fact-intensive choice of law analysis at motion to dismiss stage and deferring analysis until parties presented sufficient factual record)). Rather than performing the fact-intensive choice of law analysis, "[t]he Court may postpone a choice of law analysis yet proceed to evaluate the sufficiency of the claims on a Rule 12(b)(6) motion under the assumption that New Jersey law applies, given that Plaintiffs have argued that their common law claims are viable under New Jersey law." *Id.* (*citing Harper*, 595 F. Supp. 2d 486; *Snyder*, 792 F. Supp. 2d at 721).

Bureau, Inc., 861 F. Supp. 2d 546, 551 (E.D. Pa. 2012).

Here, Plaintiffs allege that Defendants intentionally intruded upon the Plaintiffs' solitude or private affairs or concerns without authorization, by, among other things:

- Knowingly disclosing and obtaining the children's personally identifiable information in the form of specific video materials and services requested and obtained (Complaint ¶¶ 128-130);
- Intentionally intercepting the contents of the children's electronic communications with devices that tracked and recorded their web communications, including the video materials requested and obtained (Complaint ¶¶ 137-138);
- Intentionally accessing the children's web-browsers and computing devices for purposes of tracking their Internet communications (Complaint ¶¶ 165, 170);
- Intentionally accessing, attempting to access, tampering with, altering, damaging, taking, destroying, obtaining and/or intercepting the children's computer, computer software, data, database, computer program, computer system, computer equipment and/or computer network (Complaint ¶ 190); and
- Intentionally taking the children's information from the privacy of their homes (Complaint ¶ 195).

Though some children may have voluntarily submitted personal information to Viacom when setting up accounts, none authorized Defendants (nor could they as a matter of law) to invade the privacy of their homes to intercept their private communications, track their private web browsing, or obtain and disclose their video requests and video viewing history. (Complaint ¶¶ 102, 196, 199). Defendants, however, intentionally undertook these actions "to make money" (Google Motion at 38), thereby intentionally intruding on Plaintiffs' seclusion and private affairs.

b. Defendants' Intrusions are Highly Offensive

"To establish liability for this tort, a plaintiff must show that 'the interference with the plaintiff's seclusion is a substantial one, of a kind that would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object.'" *Castro*, 384 N.J. Super. at 609 (*citing Restatement (Second) of Torts* § 652B cmt. b).

Courts have repeatedly distinguished between private content and "***noncontent*** data to which service providers must have access," finding a legitimate expectation of privacy in the former. *U.S. v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (*quoting U.S. v. D'Andrea*, 497 F. Supp. 2d 117, 120 (D. Mass. 2007)) (emphasis added); *see also U.S. v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (reasonable expectation of privacy in individuals home computers).

In *U.S. v. Forrester*, 512 F.3d 500 (9th Cir. 2008), the court explained that a URL contains private content to which a user has an expectation of privacy because "[a] URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity." *Id.* at 510 n.6 (*citing Pen Register Application*, 396 F. Supp. 2d 45, 49 (D. Mass. 2005)) ("[I]f the user then enters a search phrase [in the Google search engine], that search phrase would appear in the URL after the first forward slash. This would reveal content . . . .").

Here, even if Plaintiffs voluntarily provided their usernames and registration information (assuming children may be said to voluntarily (knowingly) submit this information), neither Plaintiffs nor their parents, authorized Defendants to intercept, track, record, and disseminate the content of their Internet communications or the videos they requested and viewed. (Complaint ¶¶ 102, 128-130,137-138,165, 170). Furthermore, Defendants admit that, in order "to make money," they intrude upon the children's private content data, with no attempt to obtain parental consent, because the practice is "long-standing, well-known, ubiquitous, and fundamental to Internet services." (Google Motion to Dismiss 38, 39). Engaging in conduct to profit off of children, with complete disregard for parental consent, is highly offensive to a reasonable person. (Complaint ¶ 197).

3. Plaintiffs State a Claim for Unjust Enrichment

"Generally, to claim unjust enrichment, a plaintiff must allege that '(1) at plaintiff's expense (2) defendant received benefit (3) under circumstances that would make it unjust for defendant to retain benefit without paying for it.'" *Snyder*, 792 F. Supp. 2d at 723-24 (*quoting In re Ford Motor Co. E-350 Van Prods. Liab. Litig.*, No. 03-4558, 2008 WL 4126264, at *63 (D.N.J. Sept. 2, 2008)). To adequately allege that the plaintiff conferred a benefit on the defendant, the plaintiff has to "allege a sufficiently direct relationship with the defendant to support the claim." *Id.* at 724 (*citing Nelson v. Xacta 3000 Inc.*, No. 08-5426, 2009 WL 4119176, at *7 (D.N.J. Nov. 24, 2009)).

Here, Plaintiffs have alleged a sufficiently direct relationship with the Defendants to support their claim. Plaintiffs were registered users of Defendant Viacom's webpages, and each Defendant placed cookies on the Plaintiffs' computing devices. (Complaint ¶¶ 4, 9-15, 103).

Moreover, at Plaintiffs' expense, and without consent from Plaintiffs' parents, Defendants intentionally and unlawfully intercepted, tracked, recorded and disclosed, *inter alia*, the children's Internet communications, videos requested, and videos viewed. (Complaint ¶¶ 77, 81, 97, 102, 128-130,137-138,165, 170). Such actions go well beyond the mere collection of "demographic information" claimed by Defendants. (Viacom Motion to Dismiss. at 38).

Defendants then utilized the intercepted information for the purpose of selling more profitable targeted advertisements. (Complaint ¶¶ 2, 37-38, 48, 71, 84). Defendant Viacom received a direct benefit from Plaintiffs' private content in the form of higher revenues from advertisers who send targeted advertisements to children. (Complaint ¶¶ 52-55). Defendant Google also received a direct benefit from Plaintiffs' private content in the form of higher revenues from children clicking on targeted advertisements, which they are more likely to do

because of their age and diminished capacity to "identify and counteract the persuasive intent of advertising." (Complaint ¶ 58). Both Defendants retained the revenues derived from such interception and dissemination of Plaintiffs' private information without any notice or compensation to the Plaintiffs or their parents. (Complaint ¶¶ 102, 157, 185, 200).

Finally, a plaintiff claiming unjust enrichment must show that "'the plaintiff expected remuneration from the defendant, or if the true facts were known to plaintiff, he would have expected remuneration from defendant, at the time the benefit was conferred.'" *Stewart v. Beam Global Spirits & Wine, Inc.*, 877 F. Supp. 2d 192, 196 (D.N.J. 2012). Here, given the higher value of children's private content data, Internet communications, and targeted advertisements directed to children (Complaint ¶¶ 49-59), had Plaintiffs known of and consented to the true facts of Defendants' conduct, they would have expected remuneration from Defendants. Thus, Plaintiffs have suffered a loss by reason of Defendants' violations including, but not limited to, violation of their rights of privacy and loss of value in their private information. (Complaint ¶ 185). It would accordingly be inequitable to allow Defendants to retain the profits from their conduct here, particularly in the absence of any parental knowledge or consent. (Complaint ¶ 201).

CONCLUSION

For all of the reasons stated herein, Plaintiffs respectfully request that this Court deny the Defendants' Motions to Dismiss.

Respectfully submitted,

/s/ Barry R. Eichen

Barry R. Eichen
Evan J. Rosenberg
EICHEN CRUTCHLOW ZASLOW &
McELROY, LLP
40 Ethel Road
Edison, NJ 08817
732-777-0100
732-248-8273 Fax
beechen@njadvocates.com
erosenberg@njadvocates.com

/s/ James P. Frickleton
James P. Frickleton
Edward D. Robertson III
BARTIMUS FRICKLETON
ROBERTSON & GOZA, PC
11150 Overbrook Rd., Suite 200
Leawood, KS 66211
913-266-2300
913-266-2366 Fax
jimf@bflawfirm.com
krobertson@bflawfirm.com

/s/ Edward D. Robertson, Jr.
Edward D. Robertson, Jr.
Mary D. Winter
BARTIMUS FRICKLETON
ROBERTSON & GOZA, PC
715 Swifts Highway
Jefferson City, MO 65109
573-659-4454
573-659-4460 Fax
chiprob@earthlink.net
marywinter@earthlink.net